Benutzerhandbuch - Deutsch

FUJITSU

FUJITSU Software ServerView Suite ServerView Event Manager

ServerView Operations Manager V7.10

Ausgabe Juni 2015

Kritik… Anregungen… Korrekturen…

Die Redaktion ist interessiert an Ihren Kommentaren zu diesem Handbuch. Ihre Rückmeldungen helfen uns, die Dokumentation zu optimieren und auf Ihre Wünsche und Bedürfnisse abzustimmen.

Sie können uns Ihre Kommentare per E-Mail an manuals@ts.fujitsu.com senden.

Zertifizierte Dokumentation nach DIN EN ISO 9001:2008

Um eine gleichbleibend hohe Qualität und Anwenderfreundlichkeit zu gewährleisten, wurde diese Dokumentation nach den Vorgaben eines Qualitätsmanagementsystems erstellt, welches die Forderungen der DIN EN ISO 9001:2008 erfüllt.

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

Copyright und Handelsmarken

Copyright © 2015 Fujitsu Technology Solutions GmbH.

Alle Rechte vorbehalten.
Lieferung nach Verfügbarkeit. Technische Änderungen vorbehalten.

Alle verwendeten Hard- und Softwarenamen sind Handelsnamen und/oder Warenzeichen der jeweiligen Hersteller.

Inhalt

1 Einleitung 9

1.1 Änderungen gegenüber der vorigen Ausgabe 10
1.2 ServerView Suite Link-Sammlung 11
1.3 Dokumentation, ServerView Suite 12
1.4 Darstellungsmittel 13

2 Event Manager 15

2.1 Erstmaliger Start 16
2.2 Event Manager starten 17
2.3 Icons 18

3 Alarm Monitor 21

3.1 Alarme ansehen 21
3.2 Alarme zu einem Server ansehen 26
3.3 Alarmeinträge filtern 26
3.4 Alarmeinträge bearbeiten 27
3.4.1 Alarme bestätigen 27
3.4.2 Alarme unterdrücken 27
3.4.3 Alarm-Unterdrückung zurücksetzen 28
3.4.4 Alarme löschen 28
3.5 Verbindung testen 29
3.6 Sonstige Einstellungen 30
3.6.1 Alarmnotiz bearbeiten 30
3.7 iRMC S2/S3-SEL- Einträge und ihre Weitergabe als SC2 MIB-Trap 31

4 Alarmkonfiguration 39

4.1 Alarmregeln 41
4.1.1 Alarmregeln verwalten 42
4.1.2 Server zuordnen 46
4.1.2.1 Serverinformation abfragen 48
4.1.3 Alarme zuordnen 50
4.1.4 Alarme weiterleiten 54

4.2 Filterregeln 58
4.2.1 Server filtern 58
4.2.2 Alarme filtern 61

4.3 Einstellungen vornehmen 63

4.4 Mail-Weiterleitung allgemein 64

4.5 Mail- und Execute-Weiterleitung an Service Provider 69

4.6 Popup-Einstellungen vornehmen 74

4.7 Pager-Einstellungen vornehmen (COM Port & Modem) 76

4.8 Execute-Einstellungen vornehmen 79

4.9 Broadcast-Einstellungen vornehmen 80

4.10 Trap-Einstellungen vornehmen 83

4.11 Makros 85

4.12 Beispiel einer Alarmkonfiguration 86

5 Traps 89

5.1 Trap-Information abfragen 89

5.2 Traps im Windows Event-Log anzeigen 92

5.3 Trapübersicht 92
5.3.1 Adaptec-Traps (Duralink.mib) 98
5.3.2 APC-Traps (Powernet.mib) 98
5.3.3 Blade System-Traps (s31.mib) 102
5.3.4 Cluster-Traps (NTCluster.mib) 107
5.3.5 DPT-Traps (dptscsi.mib) 110
5.3.6 DuplexDataManager-Traps (Ddm.mib) 113
5.3.7 DuplexWrite-Traps (DW.mib) 117

5.3.8 Festplatten-Traps (S.M.A.R.T.) (Hd.mib) 120
5.3.9 Generische Traps 121
5.3.10 MultiPath-Traps (mp.mib) 122
5.3.11 Mylex-Traps (Mylex.mib) 123
5.3.12 PCI-HotPlug-Traps (pcihotplug.mib) 129
5.3.13 PRIMEPOWER-Traps 130
5.3.14 PXRE-Traps (dec.mib) 137
5.3.15 RAID-Adapter-Traps (Megaraid.mib) 144
5.3.16 RomPilot-Traps (Rompilot.mib) 147
5.3.17 ServerControl-Traps (SC.mib) 149
5.3.18 ServerControl-Traps (SC2.mib) 156
5.3.19 ServerView-Traps (ServerView.mib) 163
5.3.20 ServerView-Status-Trap (Status.mib) 164
5.3.21 Bandlaufwerke-Traps (tapealrt.mib) 165
5.3.22 Team-Server-Traps (Fujitsu) 185
5.3.23 Threshold-Traps (Trap.mib) 189
5.3.24 USV-Traps (Upsman.mib) 196

6 MIB-Integration 199

1 Einleitung

Der ServerView Event Manager (im Folgenden kurz: Event Manager) ist eine Komponente der ServerView Suite. Diese Komponente ist nach der Installation über den ServerView Operations Manager (im Folgenden kurz: Operations Manager) verfügbar.

Der Event Manager hat eine benutzerfreundliche Web-basierte grafische Bedienoberfläche (GUI), an der Sie schnell zuverlässige und sichere Informationen über Systemfehler erhalten.

Sie können Ereignisse und Betriebszustände definieren, die Sie gemeldet bekommen wollen. Da die Verfügbarkeit der Server in einem Netzwerk von großer Bedeutung ist, werden sinnvollerweise vor allem solche Betriebszustände entsprechend konfiguriert, die diese Verfügbarkeit gefährden.

Bei Blade Systemen können Alarmmeldungen sowohl von dem gesamten Blade System als auch von den einzelnen Server Blades empfangen und angezeigt werden. Standardmäßig werden Alarme dem gesamten Blade System zugeordnet. Diese Einstellung kann in der Konfiguration geändert werden.

Der Event Manager funktioniert folgendermaßen: Ein Agent sendet einen Alarm (Trap) über das SNMP an den Event Manager, womit die Management-Station darüber informiert wird, dass ein unerwarteter Fehler aufgetreten ist. Diese können Fehlernachrichten oder Statusänderungen durch Überschreiten ausgewählter Schwellwerte sein.

Einem Trap sind verschiedene Alarmstufen zugeordnet (critical, major, minor und informational). Für jede Alarmstufe (Gewichtung) können für jeden Server einzeln Aktionen ausgewählt werden, die nach Eintreffen eines Traps ausgeführt werden sollen. Ereignisse der Alarmstufe **critical** werden immer in das Alarmprotokoll der Protokolldatei geschrieben.

Bei der Installation der Agenten können Sie festlegen, dass Alarmnachrichten an das Ereignisprotokoll von Windows gesendet werden.

1.1 Änderungen gegenüber der vorigen Ausgabe

Die vorliegende Ausgabe gilt für den Event Manager ab ServerView V7.10 und löst folgendes Online-Handbuch ab: „Event Manager“ ab ServerView V6.30, Ausgabe März 2014.

Das Handbuch wurde dem neuesten Stand der Software angepasst und bietet folgende Neuerungen:

– Ab Installation Manager V11.14.09 gibt es zwei ServerView Suite-DVDs:
  – **DVD 1: Installation** (Installation Manager)
  – **DVD 2: Management and Serviceability** (z. B. ServerView Operations Manager-Software)

  Der Abschnitt "ServerView Suite Link-Sammlung" auf Seite 11 wurde deshalb aktualisiert.

– Das Ergebnis der letzten Mail-Weiterleitung wird von ServerView Operations Manager in einer Log-Datei gespeichert, siehe Abschnitt "Mail-Weiterleitung allgemein" auf Seite 64 und Abschnitt "Mail- und Execute-Weiterleitung an Service Provider" auf Seite 69.

– Nachdem eine fremde MIB integriert wurde, muss unter Linux der Dienst **SV Services** neu gestartet werden, siehe Kapitel "MIB-Integration" auf Seite 199.

1.2 ServerView Suite Link-Sammlung

Fujitsu stellt Ihnen über die Link-Sammlung zahlreiche Downloads und weiterführende Informationen zur ServerView Suite und zu PRIMERGY Servern zur Verfügung.

Zur ServerView Suite werden Ihnen Links zu folgenden Themen angeboten:

- Forum
- Service Desk
- Handbücher
- Produktinformationen
- Sicherheitsinformationen
- Software Downloads
- Schulungen

Die Downloads umfassen u. a.:

- aktuelle Software-Stände zur ServerView Suite sowie ergänzende Readme-Dateien.
- Informationsdateien und Aktualisierungsdateien (Update Sets) für systemnahe Software-Komponenten (BIOS, Firmware, Treiber, ServerView-Agenten und ServerView-Update-Agenten) zur Aktualisierung der PRIMERGY Server anhand des ServerView Update Managers oder für den lokalen Update einzelner Server anhand des ServerView Update Managers Express.
- die aktuellen Versionen aller Dokumentationen zur ServerView Suite

Die Downloads können kostenlos vom Fujitsu Web-Server heruntergeladen werden.

Zu PRIMERGY Servern werden Ihnen Links zu folgenden Themen angeboten:

- Service Desk
- Handbücher
- Produktinformationen
- Ersatzteilkatalog

Zugriff auf die ServerView Suite-Link-Sammlung

Die Link-Sammlung der ServerView Suite erreichen Sie über verschiedene Wege:

1. Über den ServerView Operations Manager

   ► Wählen Sie auf der Startseite bzw. in der Menüzeile **Help – Links** aus.

   Anschließend wird die Startseite der ServerView Suite Link-Sammlung angezeigt.

2. über die Startseite der Online-Dokumentation zur ServerView Suite auf dem Manual-Server von Fujitsu.

   Sie gelangen auf die Startseite der Online-Dokumentation mit folgendem Link:

   http://manuals.ts.fujitsu.com

   ► Wählen Sie links in der Auswahlliste **x86 Servers**.

   ► Klicken Sie rechts unter **Selected documents** auf **PRIMERGY ServerView Links**.

   Anschließend wird die Startseite der ServerView Suite Link-Sammlung angezeigt.

3. Über die ServerView Suite DVD 2.

   ► Markieren Sie im Startfenster der ServerView Suite DVD 2 die Option **ServerView Software Produktauswahl**.

   ► Wählen Sie in der Menüleiste **Links**.

   Anschließend wird die Startseite der ServerView Suite Link-Sammlung angezeigt.

1.3 Dokumentation, ServerView Suite

Die Dokumentation ist über das Internet als Download kostenlos erhältlich. Die Online-Dokumentation finden Sie unter *http://manuals.ts.fujitsu.com* unter dem Link **x86 Servers**.

Einen Überblick über die Dokumentation, die Sie unter **ServerView Suite** finden, sowie die Ablagestruktur können Sie der ServerView Suite Sitemap (**ServerViewSuite - Site Overview**).

1.4 Darstellungsmittel

In diesem Handbuch werden folgende Darstellungsmittel verwendet:

Achtung	Mit diesem Symbol wird auf Gefahren hingewiesen, die zu Gesundheitsgefährdung, Datenverlust und Geräteschäden führen können.
	Mit diesem Symbol werden wichtige Informationen und Tipps hervorgehoben.
►	Mit diesem Symbol wird ein Arbeitsschritt, den Sie ausführen müssen, dargestellt.
halbfett	Im Fließtext werden Kommandos, Menüpunkte, Namen von Schaltflächen, Optionen, Variablen, Dateinamen und Pfadnamen **halbfett** dargestellt.
`dicktengleich`	Ausgaben des Systems werden `dicktengleich` dargestellt.
`dicktengleich halbfett`	Über die Tastatur einzugebende Anweisungen werden dicktengleich halbfett dargestellt.
Tastensymbole	Tasten werden entsprechend ihrer Abbildung auf der Tastatur dargestellt. Wenn explizit Großbuchstaben eingegeben werden sollen, so wird die Shift-Taste angegeben, z.B. SHIFT - A für A. Müssen zwei Tasten gleichzeitig gedrückt werden, so wird dies durch einen Bindestrich zwischen den Tastensymbolen gekennzeichnet.

Tabelle 1: Darstellungsmittel

Wird auf Textstellen in diesem Handbuch verwiesen, so wird die Überschrift des Kapitels bzw. Abschnitts genannt, wobei sich die Seitenangabe auf den Beginn des Abschnitts bezieht.

Bildschirmabzüge

Beachten Sie bitte, dass die Bildschirmausgaben teilweise systemabhängig sind und deshalb nicht in allen Details mit der Ausgabe auf Ihrem System übereinstimmen müssen. Ebenso können bezüglich der verfügbaren Menüpunkte systembedingte Abweichungen auftreten.

2 Event Manager

Über den Event Manager können Sie Alarmmeldungen filtern, die Anzeige festlegen und Alarmmeldungen weiterleiten.

Zur Überwachung müssen auf den verwalteten Servern ServerView-Agenten und für Server mit VMware vSphere ESXi 5 ServerView ESXi 5 CIM-Providerinstalliert werden. Tritt ein ungewöhnlicher Betriebszustand ein, dann senden die ServerView-Agenten unaufgefordert einen Alarm (Trap) an eine Management-Station. An welche Management-Stationen Traps gesendet werden, wird bei der Installation der ServerView-Agenten oder des ServerView ESXi 5 CIM-Providers festgelegt. Bei der Einrichtung des SNMP-Services auf der Management-Station wird festgelegt, von welchen verwalteten Servern Traps empfangen werden sollen.

Nach der Installation des Event Managers müssen Sie zuerst die Konfiguration für die Alarmanzeige und Alarmbehandlung vornehmen. Über die Komponente Alarm Configuration definieren Sie dazu Alarmregeln und Filterregeln. Anhand von Alarmregeln legen Sie fest, welche Alarme von welchen Servern zu welchen Zielen weitergeleitet werden sollen. Darüber hinaus können Sie über Filterregeln bestimmen, welche Alarme von welchen Servern herausgefiltert werden sollen. Eine ausführliche Beschreibung zu dieser Alarmkonfiguration finden Sie in Kapitel "Alarmkonfiguration" auf Seite 39.

In der Komponente Alarm Monitor werden die empfangenen Alarme, je nach vorgenommener Konfiguration, angezeigt. Der Alarm Monitor bietet Ihnen weitere Funktionen zur Bearbeitung der Alarmliste sowie zur zusätzlichen Filterung der Alarmanzeige. Sie können u.a. festlegen, welche Alarme von welchen Server nicht in der Alarmliste angezeigt werden. Eine ausführliche Beschreibung zum Alarm Monitor finden Sie in Kapitel "Alarm Monitor" auf Seite 21.

Mit dem Operations Manager wird eine Reihe von MIBs ausgeliefert, die in dem Event Manager integriert sind. Traps dieser MIBs können im Event Manager empfangen und bearbeitet werden. Zur Ergänzung der vorhandenen MIBs können zusätzliche fremde MIBs in den Event Manager integriert werden. Traps dieser MIBs werden nach Prüfung der MIB auch im Event Manager angezeigt.

Diese Integration erfolgt mit dem MIB Manager, der zusätzlich bei der Installation des Event Managers unter Windows bzw. Linux zur Verfügung gestellt wird. Nähere Informationen zu dem Tool finden Sie in Kapitel "MIB-Integration" auf Seite 199.

CIM-Indications für VMware vSphere ESXi 5

Ereignisse von Servern mit VMware vSphere ESXi5 werden als CIM Indications bereitgestellt. Die CIM-Indications werden vom ServerView Event Manager ausgewertet und können von ihm wie gewohnt verwaltet und weitergeleitet werden.

Über **Test Connectivity** können Sie die Verbindung zum VMware vSphere ESXi 5 Server testen (siehe Benutzerhandbuch „ServerView Operations Manager“).

Der CIM-Indication-Provider wird für die folgenden Betriebssysteme zur Verfügung gestellt:

– VMware vSphere ESXi 5

Weitere Informationen zum ServerView ESXi CIMProvider finden Sie im Handbuch „VMware-basierte PRIMERGY Server mit ServerView überwachen“.

2.1 Erstmaliger Start

Der ServerView Base Configuration Wizard enthält einen Schritt zum Konfigurieren des Event Managers (siehe Benutzerhandbuch „Base Configuration Wizard“).

2.2 Event Manager starten

Sie starten den Event Manager entweder über die Startseite des ServerView Operations Manager oder über das ServerList-Hauptfenster.

1. Starten Sie den ServerView Operations Manager.

   Wie Sie den ServerView Operations Manager starten, finden Sie in der Dokumentation zum ServerView Operations Manager.

2. Klicken Sie auf den Menüeintrag **Event Manager** entweder in der Startseite des ServerView Operations Manager oder im ServerList-Hauptfenster.

3. Starten Sie die einzelnen Komponeten des Event Managers (Alarm Monitor und Alarm Configuration) indem Sie auf den entsprechenden Link (**Alarm Monitor** oder **Alarm Configuration**) klicken.

Um den Event Manager zu starten und zu bedienen, benötigen Sie die entsprechenden Berechtigungen. Da das rollenbasierte Benutzermanagement (Role-based access control, RBAC) der ServerView Suite die Zuordnung von Berechtigungen über Benutzerrollen steuert, stellen Sie bitte sicher, dass Ihre Benutzerrolle mit den erforderlichen Rechten ausgestattet ist. Nähere Informationen finden Sie im Handbuch "Benutzerverwaltung in ServerView”.

2.3 Icons

Im Folgenden finden Sie eine Liste der Icons in den Fenstern **Alarm Monitor** und **Alarm Configuration** und deren Bedeutung.

	Alarmstufe rot: kritisch
	Alarmstufe orange: major
	Alarmstufe gelb: minor
	Alarmstufe blau: informational
	Alarmstufe grau: unbekannt
	Alarm wird ignoriert
	Für den ausgewählten Server wird der Stummschaltungsmodus mithilfe eines Zeitmodells festgelegt. Der Server befindet sich außerhalb des Zeitmodells und es ist kein Alarm eingegangen Wenn ein Alarm auftritt, wird die zugewiesene Fehlergewichtung **critical**, **major**, **minor** oder **informational** angezeigt.
	Der Alarm wurde durch eine Benutzereingabe bestätigt
	Für diesen Alarm wurde ein anderes ausführbares Programm gestartet.
	Für diesen Alarm wurde eine Broadcast-Meldung gesendet.
	Für diesen Alarm wurde eine Mail gesendet.
	Dieser Alarm löste einen Pager-Ruf aus.
	Dieser Alarm wird an die Management-Station weitergeleitet.
	Dieser Alarm wird an das lokale Betriebssystem-Event-Log weitergeleitet.

Tabelle 2: Icons im Alarm Monitor und Alarm Configuration

	grün: Pager bestätigt
	gelb: Pager abgelaufen
	rot: Pager vorhanden (arbeitet noch)
	gelb: Forwarding abgelaufen
	rot: Forwarding vorhanden (arbeitet noch)
	Tabellenspalten können nach unterschiedlichen Kriterien gefiltert werden

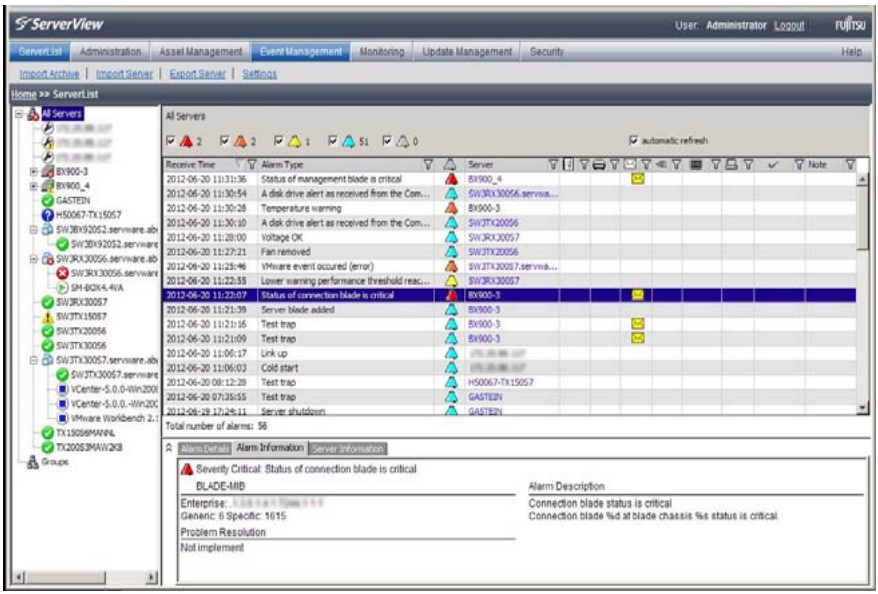
Tabelle 2: Icons im Alarm Monitor und Alarm Configuration

3 Alarm Monitor

Über die Komponente Alarm Monitor werden alle eingegangenen Alarme zu den ausgewählten Servern und Servergruppen im Hauptfenster vom Operations Manager angezeigt.

3.1 Alarme ansehen

Den Alarm Monitor starten Sie im Startfenster des Operations Managers, indem Sie unter **Event Management** auf den Link **Alarm Monitor** klicken (siehe Abschnitt "Event Manager starten" auf Seite 17). Wie Sie den Operations Manager starten, finden Sie in der Dokumentation zum ServerView Operations Manager.


ServerView
User: Administrator Logout
FUJITSU
ServerList
Administration
Asset Management
Event Management
Monitoring
Update Management
Security
Help
Import Archive | Import Server | Export Server | Settings
Home >> ServerList
All Servers
automatic refresh
Receive Time
Alarm Type
Server
Note
2012-06-20 11:31:36 Status of management blade is critical BX900_4
2012-06-20 11:30:54 A disk drive alert as received from the Com... SW3RX30056.servwa...
2012-06-20 11:30:28 Temperature warning BX900-3
2012-06-20 11:30:10 A disk drive alert as received from the Com... SW3TX20056
2012-06-20 11:28:00 Voltage OK SW3RX30057
2012-06-20 11:27:21 Fan removed SW3TX20056
2012-06-20 11:25:46 VMware event occured (error) SW3TX30057.servwa...
2012-06-20 11:22:55 Lower warning performance threshold reac... SW3RX30057
2012-06-20 11:23:07 Status of connection blade is critical BX900-3
2012-06-20 11:21:39 Server blade added BX900-3
2012-06-20 11:21:16 Test trap BX900-3
2012-06-20 11:21:09 Test trap BX900-3
2012-06-20 11:06:17 Link up
2012-06-20 11:06:03 Cold start
2012-06-20 08:12:28 Test trap H50067-TX15057
2012-06-20 07:35:55 Test trap GASTEIN
2012-06-19 17:24:11 Server shutdown GASTEIN
Total number of alarms: 56
Alarm Details
Alarm Information
Server Information
Severity Critical: Status of connection blade is critical
BLADE-MIB
Enterprise:
Generic: 6 Specific: 1615
Problem Resolution
Not implement
Alarm Description
Connection blade status is critical
Connection blade %d at blade chassis %s status is critical.
Bild 1: Alarm Monitor

Das Fenster gliedert sich in vier Bereiche:

- Die Menüleiste unterhalb der Titelzeile ermöglicht Ihnen das Navigieren zwischen folgenden Funktionen des Operations Managers:
  - Serverlist
  - Administration
  - Asset Management
  - Event Management
  - Monitoring
  - Update Management
  - Security (nur wenn OpenDS als Directory Service genutzt wird)

  In der Zeile unterhalb der Menüleiste werden jeweils je nach ausgewähltem Menü die einzelnen Menüpunkte aufgelistet.

  Weitere Informationen zu den Menüs der Menüzeile entnehmen Sie dem Benutzerhandbuch zum ServerView Operations Manager.

  Außer dem Menü Event Management sind die Menüs nur vorhanden, wenn auch der Operations Manager auf der Management-Station installiert ist.

- Der linke Bereich enthält in einer Dateibaumstruktur die Server und Servergruppen. In diesem Bereich treffen Sie die Auswahl für die Anzeige in der Alarm- bzw. Serverliste.

  Wenn Sie im Dateibaum einen Serverknoten mit dem Mauszeiger berühren, erscheint ein Tooltip. Der Inhalt des Tooltips ist von der Länge des Servernamens abhängig. Wenn der Servername im Dateibaum abgeschnitten ist, wird im Tooltip zuerst der vollständige Servername angezeigt und darunter wird dann der Servertyp aufgeführt. Wenn der Servername nicht abgeschnitten ist, enthält der Tooltip nur den Servertyp.

- Der obere rechte Bereich des Fensters enthält die Alarmeinträge zu den im Dateibaum ausgewählten Servern. Die Alarmliste ist strukturiert in Seiten.

  Anhand der Icons in der Kopfzeile des rechten Bereichs ist erkennbar, wie viele Alarmeinträge pro Alarm-Gewichtung auf einer Seite der Alarmliste vorliegen.

  Sie haben die Möglichkeit, über diese Icons die Anzeige in der Alarmliste zu steuern. Wählen Sie durch Anklicken diejenigen Alarmstufen aus, zu denen Sie Alarmmeldungen angezeigt bekommen wollen.

Über **automatic refresh** kann die Aktualisierung der Anzeige im Alarm Monitor ein- bzw. ausgeschaltet werden. Ist **automatic refresh** markiert, dann wird die Anzeige automatisch neu geladen, wenn ein Alarm protokolliert wird. Ansonsten verändert sich nur die Anzeige der protokollierten Alarme bei **Total number of alarms**.

Unterhalb der Statusleiste werden die Alarmeinträge mit folgenden Informationen angezeigt:

Receive Time
Zeitpunkt, wann der Alarm empfangen wurde.

Alarm Type
Kurzbeschreibung des Alarms.

Alarm-Icon (siehe Tabelle unten)
Gibt die Alarmgewichtung (Severity) an.

Server
Server-Name. Wenn Sie auf den Servernamen klicken, wird das Fenster **ServerView [servername]** angezeigt. Über das Fenster haben Sie die Möglichkeit, detaillierte Informationen zu dem ausgewählten Server abzufragen. Nähere Informationen dazu finden Sie im Benutzerhandbuch zum ServerView Operations Manager.

Das Fenster **ServerView [servername]** wird nur dann gestartet, wenn auch der Operations Manager auf der Management-Station installiert ist.

Forwarding-Icons (siehe Tabelle unten)
Gibt die Art der Alarmweiterleitung an.

Ack
Kennzeichnet, ob der Alarm bestätigt wurde.

Note
Anzeige einer vom Benutzer eingetragenen Notiz.

Die Icons haben folgende Bedeutung:

	Kennzeichnet die Alarmstufe.
	Der Alarm wurde in den lokalen Event-Log geschrieben.
	Dieser Alarm löste einen Pager-Ruf aus.
	Für diesen Alarm wurde eine Mail gesendet.
	Für diesen Alarm wurde eine Broadcast-Meldung gesendet.
	Für diesen Alarm wurde ein ausführbares Programm gestartet.
	Dieser Alarm wurde an die Management-Station weitergeleitet.

Tabelle 3: Icons im Alarm Monitor

- Im unteren rechten Bereich des Fensters erhalten Sie Informationen zu dem selektierten Alarmeintrag in der Alarmliste. Hierfür stehen Ihnen zwei bzw. drei Registerkarten zur Verfügung:
  - Registerkarte **Alarm Details** - enthält eine kurze Beschreibung zu dem selektierten Alarmeintrag in der Alarmliste.
  - Registerkarte **Alarm Information** - enthält detaillierte Informationen zu dem selektierten Alarmeintrag, wie sie in der MIB hinterlegt sind.
  - Registerkarte **Server Information** - liefert Informationen zu dem Server, von dem der ausgewählte Alarmeintrag stammt. Sie erhalten unter **General Information** allgemeine Informationen zu dem Server (u.a. Systemname, IP-Adresse, Community-Name) und unter **Additional Information** zusätzliche Informationen, wie sie in den Server Properties hinterlegt sind (u.a. Administrator, Ort, Modell).

    Zusätzlich finden Sie auf dieser Registerkarte einen Link in Abhängigkeit davon, ob der betreffende Server in der ServerView-Serverliste eingetragen ist oder nicht.

Ist der Server in der Serverliste vorhanden, so können Sie über den Link **Edit Server Settings** das Fenster **Server Properties** für diesen Server öffnen, über das Sie die konfigurierten Werte für den Server ändern können.

Ist der Server in der ServerView-Serverliste nicht vorhanden, dann haben Sie die Möglichkeit, über den Link **Add Server** den Server Browser zu starten und den Server in die ServerView-Serverliste aufzunehmen. Näheres zu den Server Properties und dem Server Browser entnehmen Sie dem ServerView Operations Manager Benutzerhandbuch.

Die Registerkarte **Server Information** ist nur dann vorhanden, wenn sowohl der Event Manager als auch der Operations Manager auf der Management-Station installiert sind.

3.2 Alarme zu einem Server ansehen

Wenn zu einem Server mehrere Alarmmeldungen vorliegen, dann wird in der Serverliste die höchste eingegangene Alarm-Gewichtung angezeigt. Im unteren Anzeigenbereich erhalten Sie nur Informationen zu der letzten von dieser Gewichtung eingegangenen Alarmmeldung.

Um einen Überblick über alle Alarmmeldungen zu diesem Server zu bekommen, können Sie in die Alarm-Monitor-Funktion nur für diesen Server wechseln.

Das ist einerseits möglich, indem Sie den Server im Dateibaum selektieren und die Alarm-Monitor-Funktion über die Menüzeile im Hauptfenster vom Operations Manager starten.

Eine viel schnellere Möglichkeit bietet sich Ihnen mit dem Alarm-Icon (die Alarmglocke) in der Serverliste. Klicken Sie das Alarm-Icon an, so wechseln Sie in die Alarm-Monitor-Funktion nur für diesen Server. Das bedeutet, dass in dem Listenbereich nur die Alarmmeldungen zu dem betreffenden Server vorliegen. Durch entsprechende Selektion einer Alarmmeldung in der Alarmliste können Sie zu jeder eingegangenen Alarmmeldung im Anzeigenbereich weitere Informationen abfragen.

3.3 Alarmeinträge filtern

Alarmeinträge können Sie durch Anklicken des entsprechenden Filter-Icons in der Kopfzeile der Alarmliste filtern.

Filter-Icon in der Kopfzeile der Alarmliste

Beim Anklicken des Filter-Icons öffnet sich jeweils der dazugehörige Dialog **Filtering for Column <Spaltenname>**. Treffen Sie ihre Auswahl und bestätigen Sie die Auswahl anschließend mit **OK**. Je nach Auswahl werden im Fenster dann nur die gefilterten Einträge angezeigt. Im Standard-Filter (**Standard**) werden alle Auswahlelemente über Kontrollkästchen ausgewählt. Beim kundenspezifischen Filter (**Custom**) wird die Auswahl entweder über eine direkte Eingabe oder mittels dem Stern als Platzhalter getroffen. Ein aktiver Filter wird durch ein blaues Filter-Icon angezeigt.

3.4 Alarmeinträge bearbeiten

Zum Bearbeiten der Alarmeinträge stehen Ihnen folgende Funktionen zur Verfügung:

– Alarme bestätigen
– Alarme unterdrücken
– Alarm-Unterdrückung zurücksetzen
– Alarme löschen

3.4.1 Alarme bestätigen

Sie können empfangene Alarme bestätigen.

Gehen Sie wie folgt vor:

► Wählen Sie die Alarmeinträge aus der Liste aus.

► Klicken Sie aus dem Kontextmenü den Eintrag **Ack Alarm**.

In der Spalte **Ack** wird die Bestätigung mit folgendem Icon angezeigt:

3.4.2 Alarme unterdrücken

Sie können einzelne Alarme eines Servers unterdrücken. Das ist sinnvoll, wenn die Management-Station von einem Server, der nicht korrekt läuft, mit Meldungen überhäuft wird.

Gehen Sie wie folgt vor:

► Wählen Sie die Alarmeinträge aus der Liste aus.

► Wählen Sie aus dem Kontextmenü den Eintrag **Suppress**.

Die Alarm-Unterdrückung müssen Sie bestätigen. Anschließend werden alle Alarmeinträge aus der Alarmliste gelöscht. Es werden keine Alarme dieses Typs für die betreffenden Server der Liste hinzugefügt.

Diese Einstellung können Sie über den Eintrag **Filter Settings** wieder zurücksetzen, siehe Abschnitt "Alarm-Unterdrückung zurücksetzen" auf Seite 28.

Beim Start des Servers, kann z. B. der RAID-Manager oder eine Ethernet-Netzwerkkarte einen Alarm (SNMP-Trap) als Startmeldung (z.B. RFC 1157LinkUP) ausgeben. Um diesen Alarm zu unterdrücken, müssen Sie die Alarm-Unterdrückung konfigurieren. Diese Funktion müssen Sie für jeden Server angeben. Wenn mehrere Server überwacht werden sollen, müssen Sie diese Einstellung für jeden Server der die Alarmfunktion nutzt, konfigurieren.

3.4.3 Alarm-Unterdrückung zurücksetzen

Eine bereits eingestellte Alarm-Unterdrückung können Sie wieder zurücksetzen. Gehen Sie wie folgt vor:

- Wählen Sie aus dem Kontextmenü den Eintrag **Filter Settings**.

Das Fenster **Reset suppressings** wird angezeigt, in dem alle vorher eingestellten Alarm-Unterdrückungen aufgelistet werden. Um eine Unterdrückung zurückzusetzen gehen Sie wie folgt vor:

- Markieren Sie in der Liste die entsprechende Unterdrückung.
- Klicken Sie dann auf die Schaltfläche **Delete**.
- Über die Schaltfläche **Close** schließen Sie das Fenster.

Der Eintrag wird aus der Liste entfernt und die Alarmeinstellung ist wieder aktiv.

3.4.4 Alarme löschen

Um Alarmeinträge zu löschen gehen Sie wie folgt vor:

- Wählen Sie die Alarmeinträge aus der Liste aus.
- Wählen Sie aus dem Kontextmenü den Eintrag **Delete**.

Alarme mit der Fehlergewichtung **critical** können erst gelöscht werden, wenn sie bestätigt wurden.

3.5 Verbindung testen

Zum Testen der Verbindung zu einem bestimmten Server können Sie einen Trap senden. Gehen Sie wie folgt vor:

► Wählen Sie aus dem Kontextmenü den Eintrag **Test Trap**.

Das Fenster **Test Trap** wird angezeigt:

► Wählen Sie entweder unter **Serverlist** den Server aus der Liste aus,

oder

► tragen Sie die IP-Adresse des Servers ein. Optional können Sie den Servernamen angeben.

► Übernehmen Sie die Standardwerte für **Community** und **Timeout**, oder tragen Sie die entsprechenden Werte dafür ein.

► Zum Testen der Verbindung klicken Sie auf die Schaltfläche **Test trap**.

Ein Fenster informiert Sie über den Zustand der Verbindung. Über die Schaltfläche Close schließen Sie das Fenster.

Hinweis für Linux

Wenn Sie die Verbindung des Local Host (127.0.0.1/localhost) testen, wird der Test-Trap mit einem Timeout abgebrochen. Das System wartet auf eine Antwort von der IP-Adresse des Local Host, an den der ServerView Operations Manager die Anfrage gestellt hat. Die Antwort die der Trap erhält, kommt jedoch von der realen IP-Adresse des Servers, der im SNMP-Master-Agenten festfelegt wurde.

3.6 Sonstige Einstellungen

3.6.1 Alarmnotiz bearbeiten

Die bei einem Alarmeintrag angezeigte Notiz können Sie bearbeiten:

- ► Klicken Sie auf den entsprechenden Alarmeintrag.
- ► Wählen Sie aus dem Kontextmenü den Eintrag **Edit Note**.

Das Fenster **Edit Note** wird angezeigt:

- ► Geben Sie den Text ein.
- ► Bestätigen Sie ihre Eingabe mit **OK**.

3.7 iRMC S2/S3-SEL- Einträge und ihre Weitergabe als SC2 MIB-Trap

Die folgende Aufstellung gilt für PRIMERGY Modellreihen ab Baujahr 2009.

Wenn der iRMC S2/S3 ein Ereignis in den System Event Log (SEL) schreibt, wird in einigen Fällen ein SNMP-Trap ausgelöst. Die folgende Tabelle zeigt den Zusammenhang zwischen den iRMC S2/S3-Einträgen in den SEL und den von ihnen ausgelösten Traps.

Nicht alle iRMC S2/S3-Einträge in das SEL lösen einen SNMP-Trap aus. Einige Einträge lösen den gleichen Trap aus.

Error-Code	iRMC S2/S3 SEL-Eintrag	Trap-Text	Trap-Nr.	Trap-Name
000011	System event log (SEL) warning threshold exceeded	The System Event Log for cabinet XY at server XY has exceeded XY percent of its capacity.	2101	sc2TrapMessageLogWarning
040000	'FAN XY': Fan failed	Fan 'FAN XY' failed in cabinet XY of server XY.	2014	sc2TrapFan Failed
040001	'FAN XY': Fan is working	Fan 'FAN XY' was added into cabinet XY of server XY.	2010	sc2TrapFan Added
		Fan 'FAN XY' in cabinet XY of server XY is working again.	2012	sc2TrapFanOk
040002	'FAN XY': Fan prefailure	Fan 'FAN XY' will fail in near future in cabinet XY of server XY.	2013	sc2TrapFan Critical

Tabelle 4: iRMC S2/S3-SEL-Eintrag - SC2 MIB-Trap

Error-Code	iRMC S2/S3 SEL-Eintrag	Trap-Text	Trap-Nr.	Trap-Name
040003	'FAN XY': Redundant fan failed	The redundant fan 'FAN XY' failed in cabinet XY of server XY. System can become critical if another fan in this group fails.	2015	sc2Trap RedundantFan Failed
040004	'FAN XY': Fan removed	Fan 'FAN XY' was removed from cabinet XY of server XY.	2011	sc2TrapFan Removed
050001	'Temp XY': Temperature OK	Temperature at sensor 'Temp XY' in cabinet XY of server XY is within normal range.	2020	sc2TrapTemp Ok
050016	'Temp XY': Temperature warning	Temperature at sensor 'Temp XY' in cabinet XY of server XY has reached the warning level.	2021	sc2TrapTemp Warning
050017	'Temp XY': Temperature critical	Temperature at sensor 'Temp XY' in cabinet XY of server XY has reached the critical level.	2022	sc2TrapTemp Critical
070000	'PSU XY': Power supply removed	Power supply 'PSU XY' in cabinet XY at server XY was removed.	2031	sc2TrapPower Supply Removed

Tabelle 4: iRMC S2/S3-SEL-Eintrag - SC2 MIB-Trap

Error-Code	iRMC S2/S3 SEL-Eintrag	Trap-Text	Trap-Nr.	Trap-Name
070001	'PSU XY': Power supply OK	Power supply 'PSU XY' in cabinet XY at server XY was added.	2030	sc2TrapPowerSupplyAdded
		Power supply 'PSU XY' in cabinet XY at server XY is working again.	2032	sc2TrapPowerSupplyOk
070002	'PSU XY': Power supply failed	Power supply 'PSU XY' in cabinet XY at server failed.	2034	sc2TrapPowerSupplyFailed
		Redundant power supply 'PSU XY' in cabinet XY at server XY failed. System can become critical if another power supply fails.	2035	sc2Trap RedundantPowerSupplyFailed
070003	'PSU XY': Redundand power supply AC failed	AC failure in cabinet XY of server XY.	2040	sc2TrapAcFail
070005	Power unit: power supply redundancy lost	Power supply redundancy in cabinet XY at server XY lost. System will become critical if a power supply fails.	2036	sc2TrapPowerSupplyRedundancyLost
070009	'PSU XY': Redundand power supply DC failed	DC power failure in cabinet XY of server XY.	2041	sc2TrapDcFail
070010	'PSU XY': Power supply fan failure	Fan failure at power supply 'PSU XY' in cabinet XY of server XY.	2039	sc2TrapPowerSupplyFanFailure

Tabelle 4: iRMC S2/S3-SEL-Eintrag - SC2 MIB-Trap

Error-Code	iRMC S2/S3 SEL-Eintrag	Trap-Text	Trap-Nr.	Trap-Name
07000A	'PSU XY': Power supply critical temperature	Temperature at power supply 'PSU XY' in cabinet XY of server XY has reached the critical level.	2037	sc2TrapPowerSupplyCriticalTemperature
07000F	'PSU XY': Power supply fan prefailure	Fan failure is predicted at power supply 'PSU XY' in cabinet XY of server XY.	2038	sc2TrapPowerSupplyFanFailurePrediction
0C0004	'CPU XY': CPU internal error (IERR)	Internal error (IERR) occured on CPU 'CPU XY' in cabinet XY of server XY.	2082	sc2TrapCpuIerr
0C0021	'CPU XY': Uncorrected CPU Machine Check Architecture (MCA) error			
0C0007	'CPU XY': CPU clock automatically throttled	CPU speed at server XY changed to XY percent of its maximum speed.	2080	sc2TrapCpuSpeedChanged
0C0017	'CPU XY': CPU failure predicted	CPU failure is predicted for CPU 'CPU XY' in cabinet XY.	2081	sc2TrapCpuPrefail
0C000B	'CPU XY': CPU disabled	CPU 'CPU XY' in cabinet XY of server XY is disabled.	2083	sc2TrapCpuDisabled

Tabelle 4: iRMC S2/S3-SEL-Eintrag - SC2 MIB-Trap

Error-Code	iRMC S2/S3 SEL-Eintrag	Trap-Text	Trap-Nr.	Trap-Name
120030	PCI system error (SERR): Slot 0x%1	The system wa restarted after a severe problem at cabinet XY of server XY. Nähere Informationen in der Server Management Meldungsdatei (Recovery Log).	2006	sc2TrapSevere SystemError
120031	PCI parity error (PERR): Slot 0%1			
120034	PCI bus parity error indicated by onboard device (PERR): Bus: %1 Device: 0x%2 Function: 0x%3			
120035	PCI bus system error indicated by onboard device (SERR): Bus: %1 Device: 0x%2 Function: 0x%3			
120042	CPU front side bus (FSB) error			
120047	Fatal NMI			
150000	'Voltage XY': Voltage OK	Power supply voltage 'BATT XY' in cabinet XY at server XY is within normal range again.	2050	sc2Trap VoltageOk
150030	Battery voltage 'BATT XY' OK			
150012	'Voltage XY': Voltage low critical: % Volt	Power supply voltage 'Voltage XY' in cabinet XY at server XY is too low.	2051	sc2Trap VoltageTooLo w
150032	Battery voltage 'BATT XY' low critical: % Volt			
150017	'Voltage XY': Voltage high critical: % Volt	Power supply voltage 'Voltage XY' in cabinet XY at server XY it too high.	2052	sc2Trap VoltageToo High

Tabelle 4: iRMC S2/S3-SEL-Eintrag - SC2 MIB-Trap

Error-Code	iRMC S2/S3 SEL-Eintrag	Trap-Text	Trap-Nr.	Trap-Name
150031	Battery voltage 'BATT XY' low warning: % Volt	Battery voltage 'BATT XY' in cabinet XY at server XY: Battery is predicted to fail in near future.	2054	sc2TrapBattery VoltagePrefail
190003	'DIMM XY' Memory: Uncorrectable error (ECC)	Uncorrectable memory error at module 'DIMM XY' in cabinet XY of server XY.	2065	sc2Trap Uncorrectable MemError Module
190040	'DIMM XY': Uncorrectable Parity memory error			
190007	Memory: Uncorrectable error (ECC)	Uncorrectable memory error in cabinet XY of server XY.	2067	sc2Trap Uncorrectable MemError
190008	Correctable memory error disabled	Too many correctable memory errors in cabinet XY at server XY. Error logging was disabled. If logging was disabled and not automatically enabled again, you have to reboot your server to enable memory error logging again. If logging is diabled, prefailure detection is also not active!	2071	sc2TrapMem ErrorLogging Disabled

Tabelle 4: iRMC S2/S3-SEL-Eintrag - SC2 MIB-Trap

Error-Code	iRMC S2/S3 SEL-Eintrag	Trap-Text	Trap-Nr.	Trap-Name
190017	'DIMM XY': Memory replaced by spare memory	Memory module 'DIMM XY' in cabinet XY of server XY had failed and was replaced by a hot-spare module.	2070	sc2TrapMem ErrorModule Replaced
19001A	'DIMM XY': Memory module failed predicted	Memory module failure is predicted for module 'DIMM XY' in cabinet XY of server XY.	2068	sc2TrapMem ErrorModule Prefail
19001F	Memory: redundancy lost	Memory configuration in cabinet XY of server XY has lost redundancy.	2074	sc2TrapMem Error Redundancy Lost
190035	'DIMM XY': Memory module error	Memory module 'DIMM XY' in cabinet XY of server XY is failing. Too many errors have occured.	2069	sc2Trap MemError ModuleFailing
190036	'DIMM XY': Memory module failed (disabled)			
340002	Housing opened	The front door or housing of cabinet XY was opened on server XY.	2110	sc2Trap Intrusion Assertion
340003	Housind closed	The front door of housing of cabinet XY was closed on server XY.	2111	sc2Trap Intrusion Deassertion

Tabelle 4: iRMC S2/S3-SEL-Eintrag - SC2 MIB-Trap

4 Alarmkonfiguration

Über die Komponente **Alarm Configuration** im Event Manager werden Einstellungen für die Alarmbehandlung definiert. Definiert werden Alarmregeln, Filterregeln und allgemeine Einstellungen. Die Alarmregeln legen fest, welche Alarme von welchen Servern zu welchen Zielen weitergeleitet werden (siehe Abschnitt "Alarmregeln" auf Seite 41). Die Filterregeln legen fest, welche Arten von Alarmen herausgefiltert werden (siehe Abschnitt "Filterregeln" auf Seite 58). In den allgemeinen Einstellungen wird die Behandlung von allen ankommenden und nicht herausgefilterten Alarmen festgelegt (siehe Abschnitt "Einstellungen vornehmen" auf Seite 63). Wie Sie die Komponente starten, ist in Abschnitt "Event Manager starten" auf Seite 17 beschrieben.

Nach Auswahl der Komponente **Alarm Configuration** wird folgendes Fenster angezeigt:

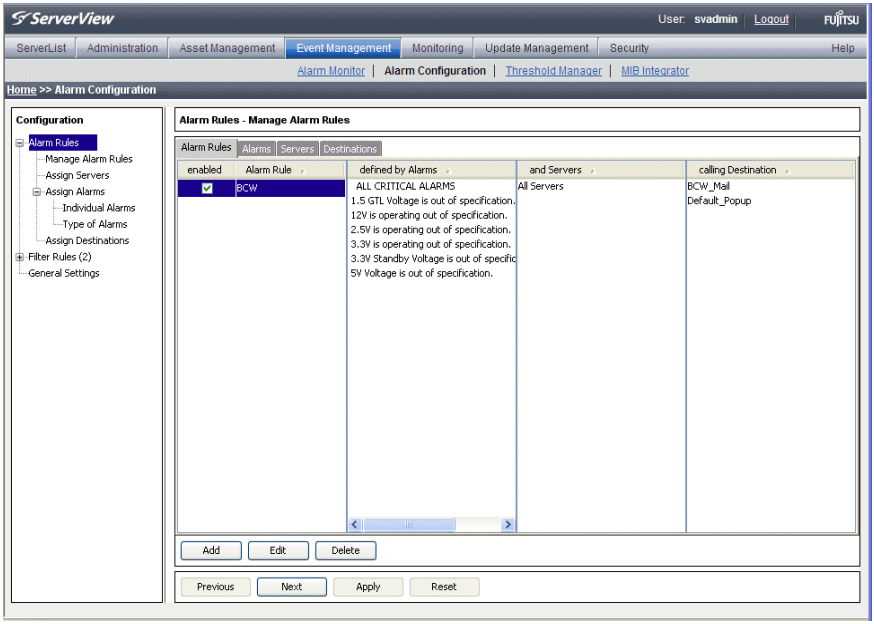


Bild 2: Alarm Configuration

Der Menübaum im linken Teil des Fensters zeigt die einzelnen Dialogfenster zur Alarmbehandlung an.

Beim ersten Aufruf wird im rechten Teil des Fensters das Dialogfenster **Alarm Rules – Manage Alarm Rules** angezeigt. Mit den Schaltflächen **Previous** und **Next** werden Sie schrittweise durch die einzelnen Dialogfenster zum Einstellen der Alarmparameter geführt. Durch Anklicken können Sie die einzelnen Dialogfenster auch direkt über den Menübaum aufrufen.

Schaltflächen

In den verschiedenen Fenstern können folgende Schaltflächen vorhanden sein:

Add
Eine neue Einstellung wird definiert.

Edit
Eine bereits vorhandene Einstellung wird verändert.

Löschen
Eine bereits vorhandene Einstellung wird gelöscht.

Zurück
Rückkehr zum vorherigen Fenster.

Übernehmen
Sichert die vorgenommenen Änderungen in die Datenbank. Nach einer vorgenommenen Änderung muss **Apply** gedrückt werden, bevor der Änderungsdialog verlassen wird. Ansonsten erscheint eine Warnmeldung.

Neustart
Die vorgenommenen Änderungen werden zurückgesetzt und es werden die Einstellungen vom vorhergehenden **Apply** aus der Datenbank übernommen.

Weiter
Das nächste Fenster wird angezeigt.

OK
Die neuen Einstellungen werden gespeichert und das Fenster wird geschlossen.

Abbrechen
Die letzten Änderungen werden nicht übernommen und das Fenster wird geschlossen.

Help
Ein Help-Text wird aufgerufen.

4.1 Alarmregeln

Eine Alarmregel leitet Alarme von verschiedenen Servern zu einem oder mehreren Zielen weiter. Eine vollständige Definition einer neuen Alarmregel besteht aus folgenden vier Schritten:

– Festlegung des Namens für die neue Alarmregel (siehe Abschnitt "Alarmregeln verwalten" auf Seite 42).

– Zuordnung von einem oder mehreren Servern zur Alarmregel (siehe Abschnitt "Server zuordnen" auf Seite 46). Nur Alarme von diesen Servern werden von der Alarmregel behandelt.

– Zuordnung von einem oder mehreren Alarmen zur Alarmregel (siehe Abschnitt "Alarme zuordnen" auf Seite 50).

– Festlegung wie auf die eintreffenden Alarme reagiert werden soll (siehe Abschnitt "Alarme weiterleiten" auf Seite 54). Hierzu können Sie Standardziele benutzen oder eigene Ziele definieren (z.B. Execute-Weiterleitung, Mail-Weiterleitung oder Mobile-Weiterleitung).

Bei der Definition einer neuen Alarmregel werden Sie schrittweise durch die einzelnen Fenster zum Einstellen der Alarmparameter geführt. Beim Verändern einer bestehenden Alarmregel können Sie die einzelnen Dialogfenster auch direkt über den Menübaum aufrufen.

4.1.1 Alarmregeln verwalten

Im Dialogfenster **Alarm Rules – Manage Alarm Rules** erhalten Sie eine Übersicht über alle definierten Alarmregeln. Die Registerkarten **Alarm Rules, Alarms, Servers** und **Destinations** ermöglichen, abhängig von der ausgewählten Registerkarte, eine unterschiedliche Sichtweise auf die definierten Alarmregeln.

Über die Schaltfläche **Add** können Sie neue Alarmregel hinzufügen. Es wird ein Fenster geöffnet, in das Sie den Namen der neuen Alarmregel eingeben können. Sie können auch Einstellungen einer bereits bestehenden Alarmregeln auf die neue Alarmregel kopieren. Wählen Sie dazu über die Auswahlliste eine bestehende Alarmregel aus. Es werden dann standardmäßig alle Einstellungen der bestehenden Alarmregel, die in den Registerkarten **Alarms, Servers, Destinations** zu sehen sind und in der Auswahlliste mit **Copy settings from rule** markiert sind, übernommen. Wollen Sie nicht von jeder Registerkarten die Einstellungen übernehmen, können Sie die einzelnen Registerkarten durch direktes Anklicken des markierten Kontrollkästchen deaktivieren. Die zugeordneten Einstellungen werden dann für die neue Alarmregel nicht übernommen.
Wollen Sie keine Einstellungen übernehmen, wählen Sie in der Auswahlliste das leere Feld aus.

Durch Anklicken der Schaltfläche **Edit** können Sie eine bestehende Alarmregel verändern. Mit der Schaltfläche **Delete** können Sie eine markierte Alarmregel löschen.

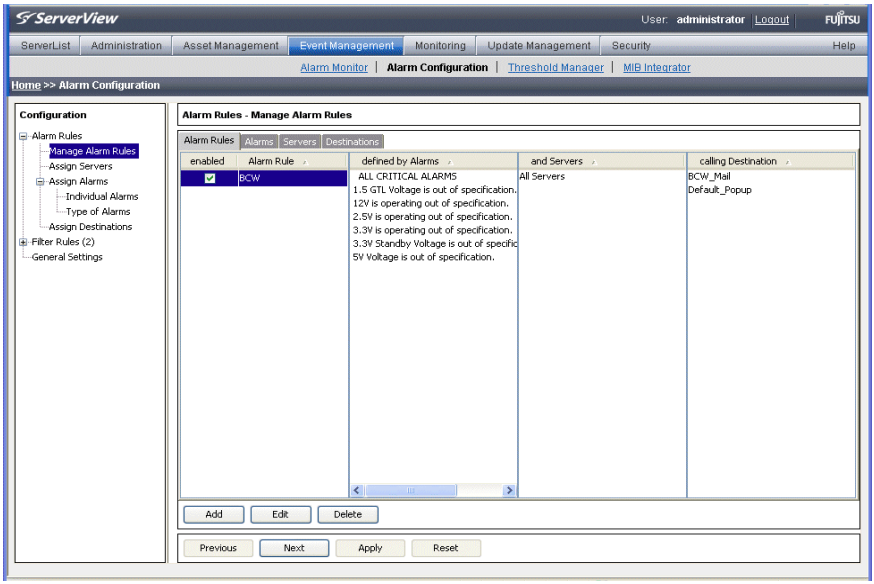


Bild 3: Alarm Rules - Manage Alarm Rules

Registerkarte **Alarm rules**

Die Registerkarte **Alarm rules** stellt eine Zuordnung von Alarmregeln zu Alarmen, Servern und Zielen der Alarme her.

Die erste Spalte listet alle bekannten Alarmregeln auf. Die Spalte **enabled** zeigt an, welche Alarmregeln aktiviert („Haken“) oder deaktiviert sind. Wenn Sie in die Spalte **enabled** klicken, kann ein „Haken“ gesetzt oder entfernt werden. Durch Anklicken der Schaltfläche **Apply** wird dann die neue Einstellung gespeichert.

Die zweite Spalte listet die Alarme auf, die der ausgewählten Alarmregel zugeordnet sind. Nur der Alarmregel zugeordnete Alarme werden weitergeleitet.

Die dritte Spalte zeigt die Server, die der ausgewählten Alarmregel zugeordnet sind. Nur Alarme von zugewiesenen Servern werden durch eine Alarmregel weitergeleitet.

Die vierte Spalte zeigt für die ausgewählte Alarmregel alle Ziele der eintreffenden Alarme an.

Über die Schaltfläche **Add** können Sie neue Alarmregeln definieren. Es wird ein Fenster ausgegeben, das Sie zur Eingabe des neuen Namens der Alarmregel auffordert. Mit der Schaltfläche **Edit** können Sie eine bestehende, ausgewählte Alarmregel verändern und mit der Schaltfläche **Delete** eine bestehende Alarmregel löschen.

Registerkarte **Alarms**

Die Registerkarte **Alarms** gibt einen Überblick, welche Alarme welchen Alarmregeln zugeordnet sind. So können Sie schnell überprüfen, ob und welches Ziel einem Alarm zugeordnet ist.

Die erste Spalte listet in alphabetischer Reihenfolge alle bekannten Alarme auf. Da die Alarme durch eine große Anzahl von unterschiedlichen Herstellern definiert werden, kann ein Name auch zweimal verwendet werden.

Die zweite Spalte listet alle Alarmregeln auf, denen der markierte Alarm zugeordnet ist.

Die dritte Spalte zeigt die Server, die der ausgewählten Alarmregel in Spalte zwei zugeordnet sind. Nur Alarme von zugewiesenen Servern werden durch eine Alarmregel weitergeleitet.

Die vierte Spalte zeigt für die ausgewählte Alarmregel alle Ziele der eintreffenden Alarme an.

Registerkarte **Servers**

Die Registerkarte **Servers** informiert darüber, welche Server von welchen Alarmregeln behandelt werden. Hier können Sie überprüfen, ob Alarme von einem Server zumindest an ein Ziel weitergeleitet werden.

Die erste Spalte listet in alphabetischer Reihenfolge alle bekannten und nicht herausgefilterten Server auf (siehe Abschnitt "Server filtern" auf Seite 58). Durch Anklicken wählen Sie den Server aus, zu dem Sie weitere Informationen haben möchten.

Die zweite Spalte listet alle Alarmregeln auf, denen der ausgewählte Server zugeordnet ist.

Die dritte Spalte gibt die Alarme aus, die der ausgewählten Alarmregel zugeordnet sind.

Die vierte Spalte enthält alle Ziele, zu denen die ausgewählte Alarmregel die eintreffenden Alarme weiterleitet.

Registerkarte **Destinations**

Die Registerkarte **Destinations** informiert darüber, an welches Ziel mit welchen Alarmregeln weitergeleitet wird.

Die erste Spalte listet alle bekannten Ziele in alphabetischer Reihenfolge auf.

Die zweite Spalte listet alle Alarmregeln auf, die die eintreffenden Alarme an das ausgewählte Ziel weiterleiten.

Die dritte Spalte enthält die Liste der Server, die der ausgewählten Alarmregel zugeordnet sind.

Die vierte Spalte zeigt alle Alarme, die der ausgewählten Alarmregel zugeordnet sind.

In der Registerkarte **Destinations** können Sie über die Schaltflächen **Add** ein neues Ziel festlegen, über die Schaltfläche **Edit** ein bestehendes Ziel verändern und mit der Schaltfläche **Delete** ein bestehendes Ziel löschen. Die Ziele **Default_Popup** und **Event_Log** können nicht gelöscht werden. Das Ziel **Event_Log** kann auch nicht verändert werden.

4.1.2 Server zuordnen

Im Dialogfenster **Alarm Rules - Assign Servers** legen Sie die Server und/oder Servergruppen fest, die einer Alarmregel zugeordnet werden sollen.

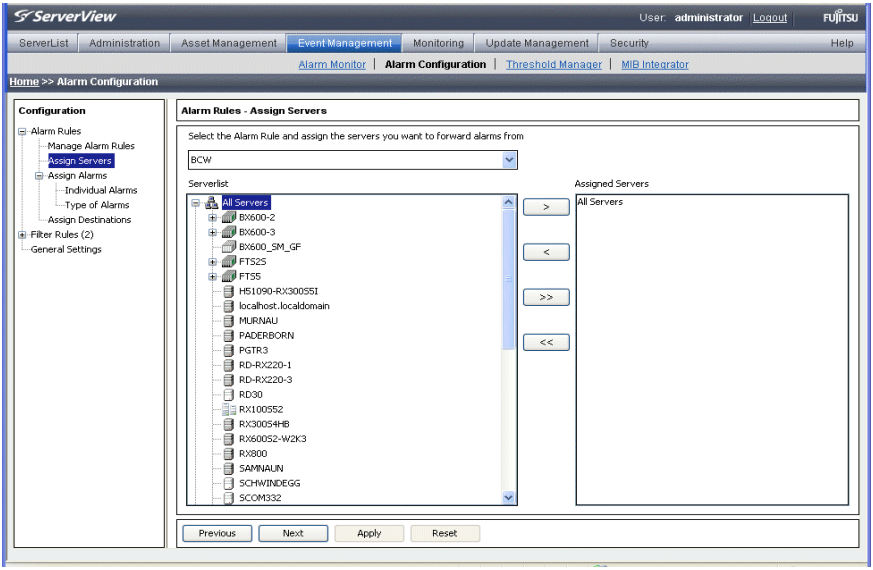


Bild 4: Alarm Rules - Assign Servers

Über die Auswahlliste können Sie die Alarmregel auswählen, die Sie bearbeiten möchten. Der Dateibaum im Fenster **Serverlist** enthält alle bekannten und nicht herausgefilterten Server. Im Fenster **Assigned Servers** wird die Liste der Server und Servergruppen ausgegeben, die der Alarmregel zugeordnet sind.

Wenn Sie eine Servergruppe nach **Assigned Servers** verschieben, werden zugehörige Untergruppen nicht mitverschoben.Diese Untergruppen müssen Sie extra verschieben. Diese Einschränkung gilt nicht für **All Servers**.

Da verschiedene Servergruppen gleich heißen können, werden sie in der Komponente **Alarm Configuration** zusammen mit ihrer Gruppen-Hierarchie ausgegeben.

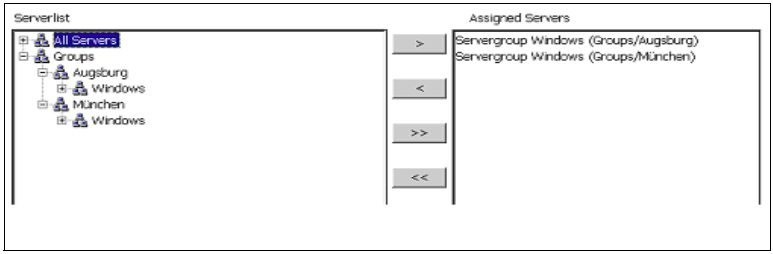


Bild 5: Alarm Rules - Assign Servers-Gruppen-Hierarchie

Mit folgenden Schaltern können Sie festlegen, welche Server zu dieser Alarmregel gehören sollen:

>

Die ausgewählten Server werden der Alarmregel hinzugefügt.

<

Die ausgewählten Server werden aus der Alarmregel entfernt.

>>

Alle bekannten Server werden der Alarmregel hinzugefügt.

<<

Alle Server werden aus der Alarmregel entfernt.

Wählen Sie im Kontextmenü den Eintrag **Show Information about Server**, werden zusätzliche Informationen zu dem ausgewählten Server angezeigt. Wählen Sie den Menüpunkt **Show unassigned servers only,** werden in der Serverliste nur die Server ausgegeben, die noch keiner Alarmregel zugeordnet sind. Durch die Auswahl des Menüpunktes **Show all Servers** werden wieder alle Server angezeigt.

Durch Anklicken der Schaltfläche **Apply** werden die neuen Einstellungen gespeichert. Wenn Sie die Schaltfläche **Reset** anklicken, werden wieder die Einstellungen der letzten Speicherung übernommen.

Wenn Sie das Fenster verlassen, ohne die geänderte Konfiguration zu speichern, oder wenn notwendige Elemente der Alarmregel fehlen, wird eine entsprechende Fehlermeldung ausgegeben.

4.1.2.1 Serverinformation abfragen

Wählen Sie im Kontextmenü den Eintrag **Show Information about Server** aus, öffnet sich das Fenster **Server information** und Sie erhalten zusätzliche Informationen über den ausgewählten Server.

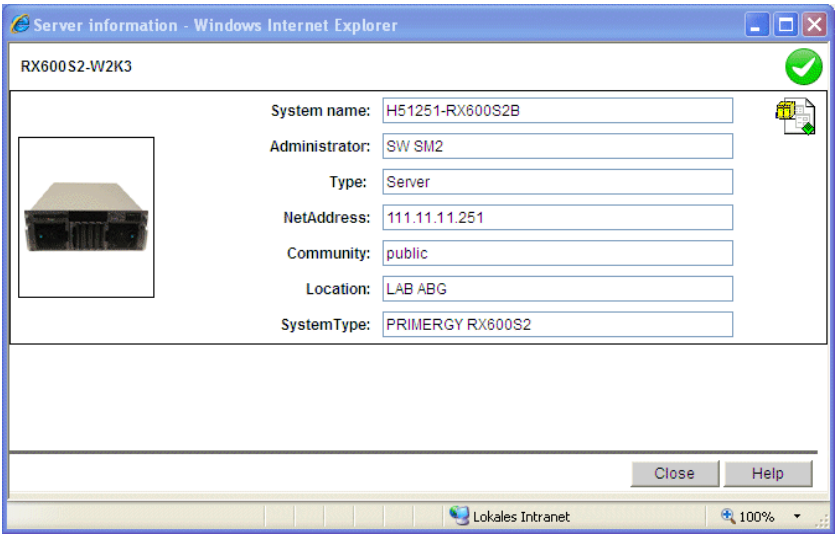


Bild 6: Server-Information

Der Kopfzeile entnehmen Sie den Namen des Servers und den aktuellen Betriebszustand (anhand des Status-Icons).

Unterhalb des Status-Icons finden Sie ein weiteres Icon, das Sie darüber informiert, ob der Server in der Serverliste eingetragen ist oder nicht:

Der Server ist bekannt, d.h. der Server ist in der ServerView Serverliste vorhanden.

Der Server ist nicht bekannt, d.h. der Server ist nicht in der ServerView Serverliste vorhanden.

Wenn der Server in der Serverliste vorhanden ist, so wird die Information zum Server angezeigt. Wenn ein Server nicht in der Serverliste eingetragen ist, aber sein aktueller Status **manageable** ist, holt sich der Event Manager die Information von dem Server direkt.

Sie haben die Möglichkeit, den Operations Manager für den ausgewählten Server über dieses Fenster zu starten. Dazu klicken Sie auf das Status-Icon ganz oben rechts.

Die Statusanzeige, das Bild des Servers und die Möglichkeit, den Operations Manager zu starten, werden nur unterstützt, wenn der Operations Manager installiert ist.

Mit **Close** schließen Sie das Fenster **Server information**.

4.1.3 Alarme zuordnen

Im Dialogfenster **Alarm Rules – Assign Alarms** können Sie im Dialogfenster **Individual Alarms** die Alarme für die Alarmregel festlegen und sich alle Informationen über die zugeordneten Alarme anzeigen lassen. Im Dialogfenster **Type of Alarms** können Sie für ausgewählte Alarmregeln festlegen, welche Art von Alarmen weiterleitet werden sollen.

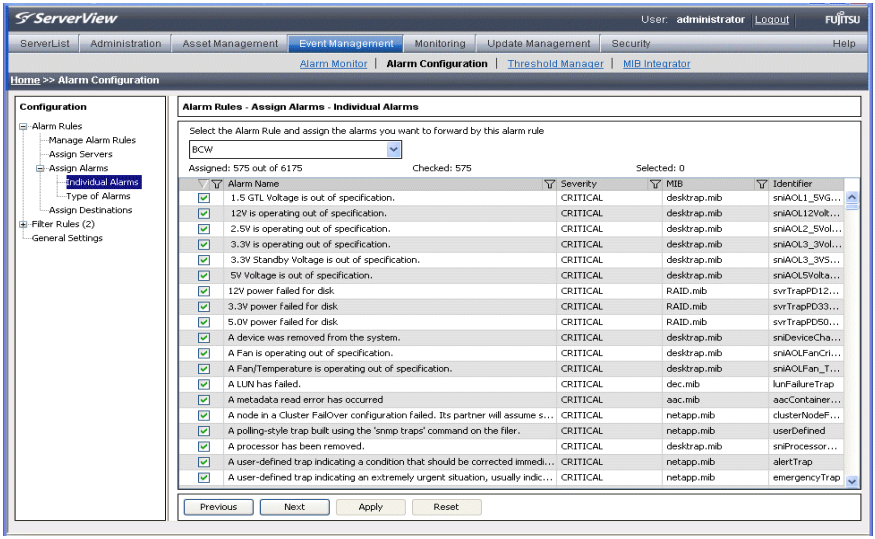


Bild 7: Alarm Rules - Assign Alarms - Individual Alarms

Im Dialogfenster **Individual Alarms** werden in der oberen Auswahlliste die Namen aller bekannten Alarmregeln aufgelistet. Hier können Sie die Alarmregel auswählen, die Sie bearbeiten wollen.

Tritt ein unbekannter Alarm ein, können Sie diesem eine Alarmregel zuordnen. Stellen Sie dazu sicher, dass unbekannte Alarme nicht unterdrückt, sondern zugelassen werden. Zulassen können Sie unbekannte Alarme über die Filtereinstellungen im Dialogfenster **Filter Rules – Alarm Filtering** (siehe "Alarme filtern" auf Seite 61). Zusätzlich müssen Sie im Dialogfenster **Alarm Rules – Assign Alarms – Type of Alarms** das dazugehörige Kontrollkästchen aktivieren.

Der Zähler **Assigned** gibt sowohl die Anzahl der Alarme an, die aktuell dieser Alarmregel zugeordnet sind, als auch die Anzahl aller bekannten Alarme.

Der Zähler **Checked** zählt alle Alarme, deren Kontrollkästchen markiert sind. Ob die Alarme gefiltert wurden, wird dabei nicht berücksichtigt.

Der Zähler **Selected** gibt die Anzahl der aktuell aus der Alarmliste ausgewählten Alarme an.

Die Alarmliste im unteren Bereich des Fensters zeigt mit Hilfe von Kontrollkästchen an, welche Alarme der Alarmregel zugeordnet sind. Ebenso werden die Namen der Alarme (**Alarm Name**), ihre Gewichtung (**Severity**) sowie ihre MIB-Datei (**MIB**), in der dieser Alarm definiert ist, und ihr Trap-Name (**Identifier**) angezeigt.

Alarme, die der ausgewählten Alarmregel zugeordnet sind, sind durch markierte Kontrollkästchen gekennzeichnet. Durch direktes Anklicken kann ein Kontrollkästchen markiert oder eine bestehende Markierung zurückgenommen werden.
Durch Anklicken der Schaltfläche **Apply** werden die geänderten Einstellungen der Alarmregel gespeichert. Der Wert des Zählers **Assigned** entspricht dann dem Wert des Zählers **Checked**.

Alle Alarme der Alarmliste können sortiert oder nach unterschiedlichen Kriterien gefiltert werden. So ist es möglich, nur bestimmte Alarme anzuzeigen.

Sortiert wird durch Anklicken der entsprechenden Spalte in der Kopfzeile der Alarmliste. Es kann alphabetisch nach **Alarm Name**, **Severity**, **MIB** oder **Identifier** sortiert werden.

Gefiltert wird durch Anklicken des entsprechenden Filter-Icons in der Kopfzeile der Alarmliste
Die Alarme können nach markierten Alarmen (markierte Kontrollkästchen)**, Alarm Name, Severity** oder **MIB** gefiltert werden. Beim Anklicken des Filter-Icons öffnet sich jeweils das dazugehörige Dialogfenster. Wenn Sie beispielsweise **Severity** gewählt haben, werden im Dialogfenster die Fehlergewichtungen angezeigt, die Sie dann auswählen können. Treffen Sie ihre Auswahl und bestätigen Sie die Auswahl anschließend mit **OK**. Je nach Auswahl werden im Fenster dann nur die gefilterten Alarme angezeigt. Ein aktiver Filter wird durch ein blaues Filter-Icon angezeigt.

Im Standard-Filter (**Standard**) werden alle Auswahlelemente über Kontrollkästchen ausgewählt. Beim kundenspezifischen Filter (**Customize**) wird die Auswahl entweder über eine direkte Eingabe (z.B. MINOR) oder mittels dem Stern als Platzhalter getroffen. Bei Severity werden zum Beispiel bei Angabe von M* die Gewichtungen Major und Minor ausgewählt.

Die Alarmliste bietet ein Kontextmenü an, in diesem Kontextmenü können Sie über den Eintrag:

Show information about selected Alarm
zusätzliche Informationen zu dem ausgewählten Alarm erhalten

Check all alarms
alle momentan bekannten Alarme der Alarmregel hinzufügen

Check selected alarm(s)
die ausgewählten Alarme der Alarmregel hinzufügen

Uncheck all alarms
alle momentan bekannten Alarme aus der Alarmregel entfernen

Uncheck selected alarm(s)
die ausgewählten Alarme aus der Alarmregel entfernen

Durch Anklicken der Schaltfläche **Apply** werden die neuen Einstellungen gespeichert. Wenn Sie die Schaltfläche **Reset** anklicken, werden wieder die Einstellungen der letzten Speicherung übernommen.

Im Dialogfenster **Alarm Rules – Assign Alarms – Type of Alarms** können Sie für ausgewählte Alarmregeln festlegen, welche Alarme weiterleitet werden sollen.

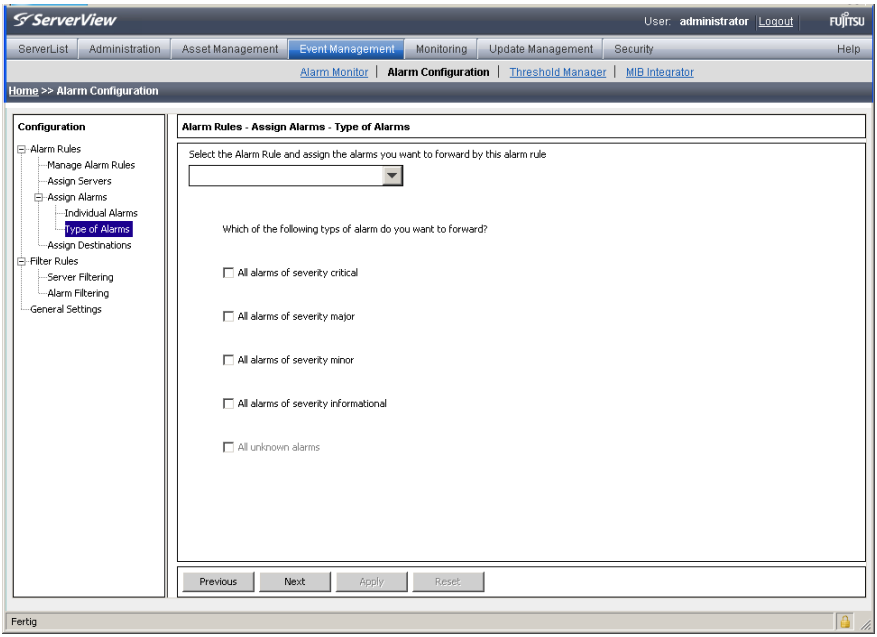


Bild 8: Alarm Rules - Assign Alarms - Type of Alarms

Die obere Auswahlliste listet Ihnen die Namen von allen bekannten Alarmregeln auf. Hier können Sie die Alarmregel auswählen, die Sie bearbeiten wollen. Sie können folgende Filtereinstellungen ein- bzw. ausschalten:

All alarms of severity critical

Alle Alarme der Fehlergewichtung **critical** werden entsprechend der Alarmregel behandelt.

All alarms of severity major

Alle Alarme der Fehlergewichtung major werden entsprechend der Alarmregel behandelt.

All alarms of severity minor

Alle Alarme der Fehlergewichtung **minor** werden entsprechend der Alarmregel behandelt.

All alarms of severity informational

Alle Alarme der Fehlergewichtung **informational** werden entsprechend der Alarmregel behandelt.

All unknown alarms

Alle unbekannten Alarme werden entsprechend der Alarmregel behandelt.

4.1.4 Alarme weiterleiten

Im Dialogfenster **Alarm Rules – Assign Destinations** können Sie die Einstellungen bezüglich der Ziele von Alarmen vornehmen. Wählen Sie eine Alarmregel aus und definieren Sie anschließend die Aktionen, die für die Server dieser Alarmregel bei bestimmten Alarmmeldungen ausgelöst werden sollen.

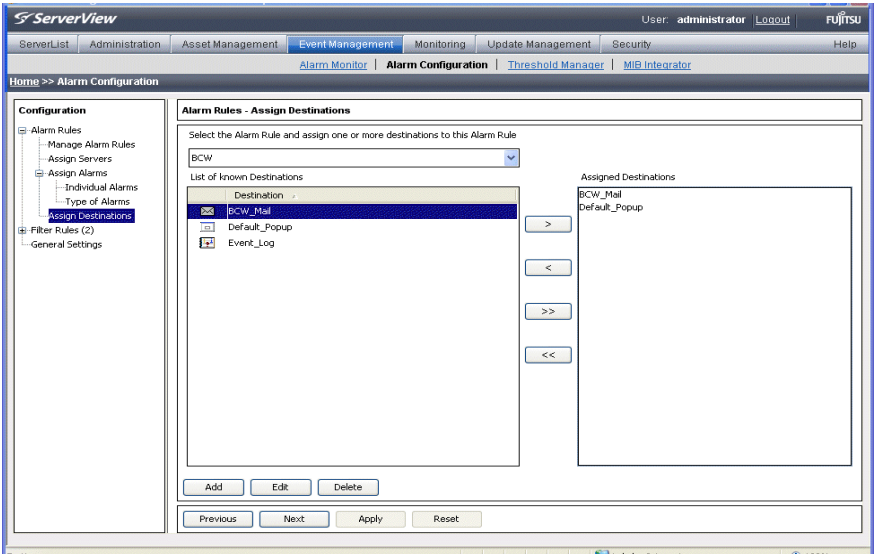


Bild 9: Alarm Rules - Assign Destinations

Die obere Auswahlliste listet Ihnen die Namen von allen bekannten Alarmregeln auf. Hier können Sie die Alarmregel auswählen, die Sie bearbeiten wollen. Im Fenster **List of known Destinations** stehen alle bekannten Ziele. Im Fenster **Assigned Destinations** wird die Liste der Ziele ausgegeben, die der Alarmregel zugeordnet sind.

Über die Schaltfläche **Add** können Sie ein neues Ziel festlegen, über die Schaltfläche **Edit** ein bestehendes Ziel verändern und mit der Schaltfläche **Delete** ein bestehendes Ziel löschen.
Das Ziel **Automatic Service Mail** kann weder gelöscht noch in das Fenster **Assigned Destinations** geschoben werden.

Mit folgenden Schaltern können Sie die Weiterleitung eines Alarms ein- bzw. ausschalten:

>
Die ausgewählten Ziele werden eingeschaltet.

<
Die ausgewählten Ziele werden ausgeschaltet.

>>
Alle bekannten Ziele werden eingeschaltet.

<<
Alle bekannten Ziele werden ausgeschaltet.

Durch Anklicken der Schaltfläche **Apply** werden die neuen Einstellungen gespeichert. Wenn Sie die Schaltfläche **Reset** anklicken, werden wieder die Einstellungen der letzten Speicherung übernommen.

Sie können für die Alarmegel festlegen, ob:

– eine Mail versendet werden soll (**Mail**)

– eine Meldung ausgegeben wird (**Popup**)

– der Alarm protokolliert werden soll (**Event Log**)

– ein Anruf auf einem Pager (Cityruf) oder Handy ausgelöst werden soll (**Pager**)
(Diese Einstellung ist für den japanischen Markt nicht verfügbar.)

– ein ausführbares Programm gestartet werden soll (**Execute**)

– eine Broadcast-Meldung ausgelöst werden soll (**Broadcast**)

– ein Trap erzeugt werden soll, der an eine andere Management-Station weitergeleitet wird (**Station**)

– eine Mail an eine spezielle Service-Adresse versendet werden soll (**Automatic Service Mail**)
(Diese Einstellung ist für den japanischen Markt nicht verfügbar.) Für den japanischen Markt wird eine andere Weiterleitung, genannt FJJ Service Mail, zur Verfügung gestellt.)

Durch Anklicken der Schaltfläche *Add* können Sie ein neues Ziel festlegen. Es wird nachfolgendes Fenster mit den verfügbaren Zielen geöffnet.

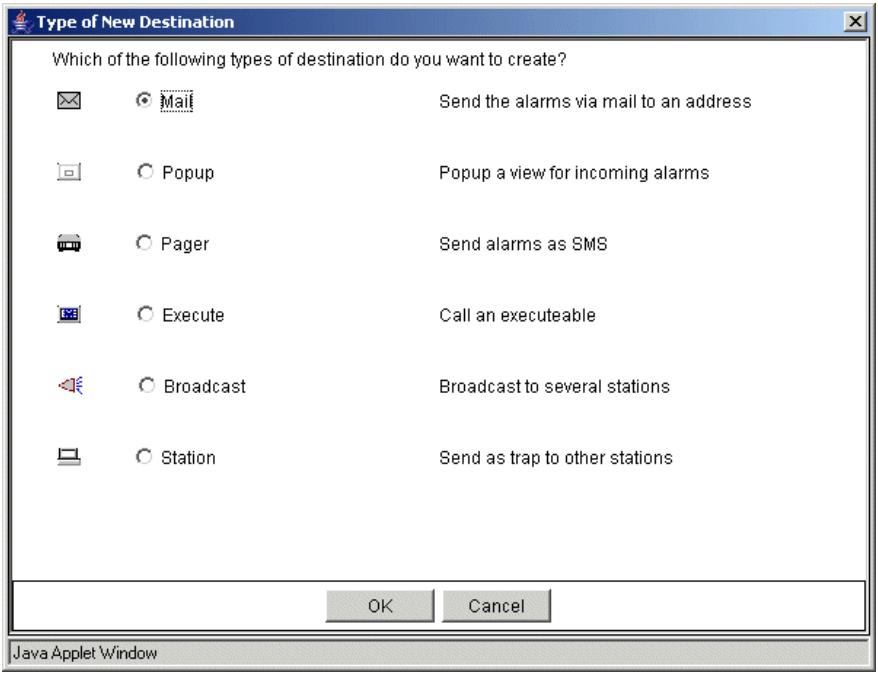


Bild 10: Type of New Destination

Durch Anklicken der Schaltfläche **OK** werden je nach Auswahl zusätzliche Fenster angezeigt, in denen Sie weitere Einstellungen vornehmen müssen. Über unterschiedliche Registerkarten können dort alle zur Weiterleitung notwendigen Parameter definiert werden. Eine detaillierte Beschreibung zu den Fenstern erhalten Sie jeweils über die Schaltfläche Help. Weitere Informationen zu den einzelnen Fenstern entnehmen Sie den nachfolgenden Abschnitten zu den entsprechenden Weiterleitungen und Einstellungen ab Seite 64.

- Hinweis für SMTP AUTH

  Zum Versenden von Mails wird **SMPT AUTH** unterstützt. Die unterstützte Authentifizierungsmethode ist: CRAM MD5 / LOGIN / PLAIN. Die Authentifizierungsmethode, die Sie benutzen, wenn Sie eine Mail verschicken, schaltet automatisch zur sichersten Authentifizierungsmethode um. Diese Methode ist kompatibel zur Authentifizierungsmethode, welche vom ausgewählten Server (Destination Server) unterstützt wird.

  Wenn die Eingabefelder **User** und Password nicht belegt sind, werden die Mails von SMPT ohne Authentifizierung verschickt.

- Wenn Sie **Mail** für das Weiterleiten ausgewählt haben, wird der Zeichensatz (**charset**) in Mails für **Subject** und Message folgendermaßen gesetzt:
  - an einer Windows basierten Management-Station **charset=Shift-JIS**
  - an einer Linux basierten Management-Station charset= **UTF-8**

4.2 Filterregeln

Die Filterregeln legen fest, von welchen Servern oder Servergruppen Sie Alarme ignorieren wollen (siehe Abschnitt "Server filtern" auf Seite 58) und/oder welche Alarme ignoriert werden sollen (siehe Abschnitt "Alarme filtern" auf Seite 61).

Filterregeln haben eine höhere Priorität als Alarmregeln. Wenn ein Alarm aufgrund der Filterregeln ignoriert wird, wird die Alarmregel, die dem Alarm zugeordnet ist, nicht aktiviert.

4.2.1 Server filtern

Im Dialogfenster **Filter Rules – Server Filtering** legen Sie fest, von welchen Servern oder Gruppen von Servern Sie die Alarme herausfiltern wollen.

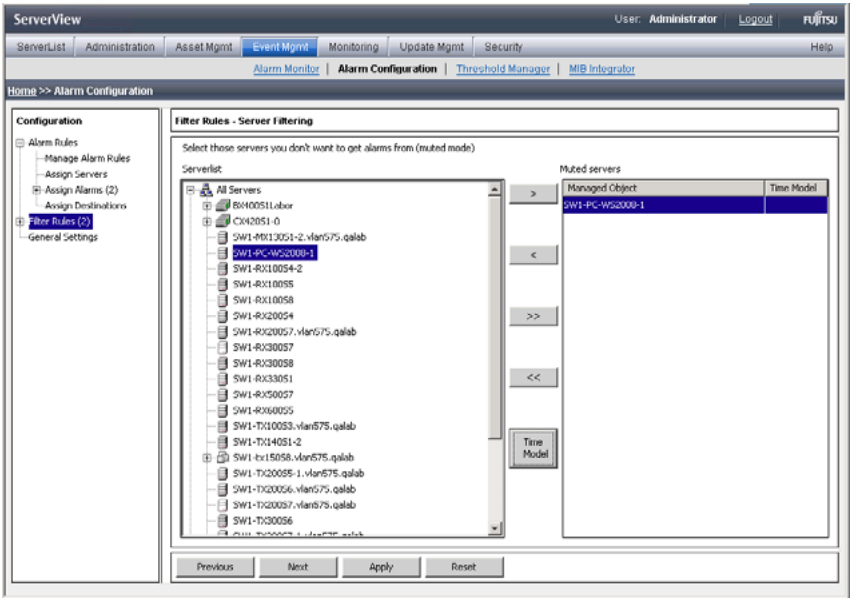


Bild 11: Server Filtering screen

Läuft der Event Manager auf einem Server und sind in der Serverliste keine weiteren Server vorhanden, so wird automatisch dieser Server als local host angezeigt. Weitere Einstellungen dazu sind nicht notwendig.

Im Fenster **Serverlist** werden alle Server und Servergruppen der Serverliste angezeigt. Im Fenster **Suppress from handling** werden die Server oder Servergruppen angezeigt, deren Alarme nicht behandelt werden sollen.
Mit folgenden Schaltern können Sie die Server filtern:

>

Die Alarme der ausgewählten Server oder Servergruppen sind stummgeschaltet.

<

Die Alarme der ausgewählten Server oder Servergruppen werden weitergeleitet.

>>

Alle Alarme der Server oder Servergruppen aus der Serverliste sind stummgeschaltet.

<<

Alle Alarme der Server oder Servergruppen im Fenster **Muted servers** werden wieder verarbeitet. Alle eintreffenden Alarme der Server oder Servergruppen der Serverliste werden weitergeleitet.

Mit der Schaltfläche **Time Model** können Sie Zeitmodelle für die gefilterten Server oder Servergruppen im Fenster **Muted servers** festlegen, sodass sie für einen bestimmten Zeitraum stummgeschaltet sind und außerhalb dieses Zeitraums verarbeitet werden.

- Wählen Sie im Fenster **Muted servers** den Server oder die Servergruppe aus, für den bzw. die Sie ein Zeitmodell festlegen möchten.
- Klicken Sie auf die Schaltfläche **Time Model**.
- Der Dialog **Server Filtering** - **Time Model Settings** wird angezeigt.

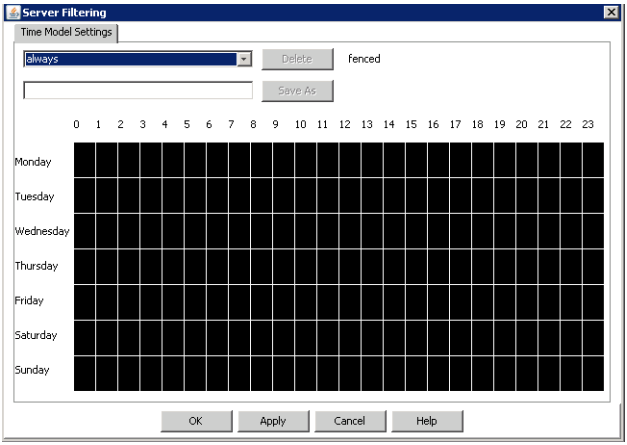


Bild 12: Dialogfenster Server Filtering - Time Model

– Aus der Auswahlliste können Sie ein vordefiniertes Zeitmodell auswählen.

Sie können die vordefinierten Zeitmodelleinstellungen einzeln ändern, mit Ausnahme von **always** und **never**, und diese Änderungen dann mit der Schaltfläche **Save As** unter einem neuen Zeitmodellnamen speichern. Sie können stundenweise für die ganze Woche festlegen, wann ein Alarm stummgeschaltet werden soll.

Klicken Sie im Dialog **Time Model Settings** auf die Schaltfläche **Apply**, um die neuen Einstellungen zu speichern. Wenn Sie die Schaltfläche **Cancel** anklicken, werden wieder die Einstellungen der letzten Speicherung übernommen.

Wenn Sie eine definierte Zeitmodelleinstellung entfernen möchten, wählen Sie die vordefinierte Zeitmodelleinstellung **always** aus dem Dropdown-Menü im Dialog **Time Model Settings** aus. Dadurch wird die definierte Zeitmodelleinstellung entfernt und die Spalte **Time Model** im Fenster **Muted servers** im Bildschirm **Server Filtering** wird gelöscht.

Wählen Sie im Fenster **Serverlist** des Bildschirms **Server Filtering**einen Server aus und wählen Sie aus dem Kontextmenü die Option **Show Information about Server**, um zusätzliche Informationen zum Server anzuzeigen.

Klicken Sie im Dialog **Server Filtering** auf die Schaltfläche **Apply**, um die neuen Einstellungen zu speichern. Wenn Sie die Schaltfläche **Reset** anklicken, werden wieder die Einstellungen der letzten Speicherung übernommen.

4.2.2 Alarme filtern

Im Dialogfenster **Filter Rules – Alarm Filtering** können Sie Filtereinstellungen für einen Alarmtyp ein- bzw. ausschalten.

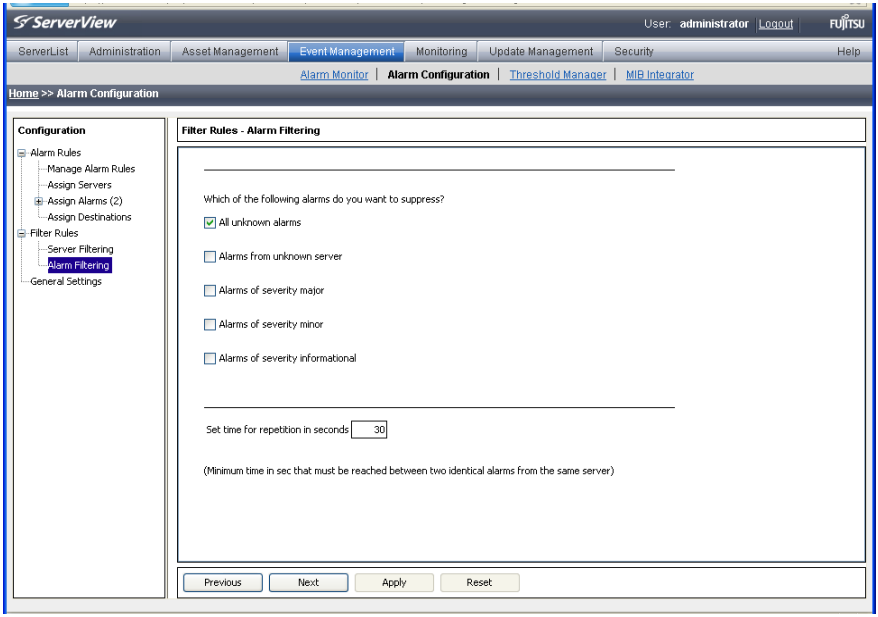


Bild 13: Filtereinstellung für Alarmtyp

Sie können folgende Filtereinstellungen ein- bzw. ausschalten:

All unknown alarms
: Unbekannte Alarme herausfiltern. Unbekannte Alarme sind Alarme, die in keiner der integrierten MIBs definiert sind.

Alarms from unknown server
: Alarme von unbekannten Servern herausfiltern.

Alarms of severity major
: Nach der entsprechenden Fehlergewichtung **major** filtern.

Alarms of severity minor
: Nach der entsprechenden Fehlergewichtung **minor** filtern.

Alarms of severity informational
: Nach der entsprechenden Fehlergewichtung **informational** filtern.

Im Eingabefeld **Set time for repetition in seconds** können Sie die Zeit festlegen, nach der der gleiche Alarm vom gleichen Server wieder durchgelassen wird. Das ist sinnvoll, damit die Management-Station nicht mit gleichen Alarmen überhäuft wird, die von einem nicht korrekt laufenden Server geliefert werden.

Wenn Sie zum Beispiel ein Intervall von 30 Sekunden festlegen, haben die einzelnen Gewichtungen die nachfolgenden Filter-Intervalle:

Severity of alarm	**Value of severity**	**Expression from which filter interval is requested**	**Filter interval**
Kritische	1	30 seconds × 1	30 seconds
Schwerer Fehler	2	30 seconds × 2	60 seconds
Leichter Fehler	3	30 seconds × 3	90 seconds
Information	4	30 seconds × 4	120 seconds

Tabelle 5: Filter interval of each severity

4.3 Einstellungen vornehmen

Im Dialogfenster **General Event Configuration Settings** können Sie allgemeine Einstellungen für die Behandlung der Alarme definieren.

Sie können die Aktionen festlegen, die standardmäßig und unabhängig von den Alarmgruppen beim Eintreffen eines Alarms ausgeführt werden sollen.

Folgende Aktionen können Sie festlegen:

- Alarme zu einer fehlgeschlagenen Authentifizierung werden unterdrückt.
- Alarme von Server-Blades werden mit dem entsprechenden Namen des Blade-Servers ausgegeben.

Für verschiedene Fehlergewichtungen können Sie folgende Aktionen festlegen. Beliebige Kombinationen sind möglich.

- der Alarm soll in die Event-Log-Liste des Betriebssystems geschrieben werden.

  Wenn Sie Alarme mit den entsprechenden Fehlergewichtungen empfangen, werden diese Alarme in die Event-Log-Liste des Betriebssystems geschrieben.

- der Alarm soll in eine Popup-Meldung auf der Management-Station ausgegeben werden.Wenn Sie Alarme mit den entsprechenden Fehlergewichtungen empfangen, wird für jeden dieser Alarme eine Popup-Meldung auf der Management-Station ausgegeben.

- das Fenster des Alarm Monitors soll in den Vordergrund geholt werden.

  Jedes Mal, wenn Sie einen Alarm mit der entsprechenden Fehlergewichtung empfangen, wird das Fenster des Alarm Monitors in den Vordergrund geholt. Dazu muss der Alarm Monitor bereits gestartet sein.

Sie können angeben, wann der Alarm gelöscht werden soll. Sie können festlegen, ob der Alarm gelöscht werden soll, wenn er ein bestimmtes Alter erreicht hat oder wenn eine bestimmte Anzahl von Einträgen in der Log-Liste enthalten ist. Ist eine bestimmte Anzahl von Einträgen in der Liste erreicht, wird der älteste Eintrag dieser Liste gelöscht.

Durch Anklicken der Schaltfläche **Apply** werden die neuen Einstellungen gespeichert. Wenn Sie die Schaltfläche **Reset** anklicken, werden wieder die Einstellungen der letzten Speicherung übernommen.

Mit den allgemeinen Einstellungen werden die Event-Logs unabhängig von den Alarmregeln aufgezeichnet. Somit können, abhängig von der Konfiguration, zwei Event-Logs für den gleichen Alarm aufgezeichnet werden.

4.4 Mail-Weiterleitung allgemein

Mail-Einstellungen vornehmen

Wenn Sie **Mail** für das Weiterleiten ausgewählt haben, erscheint nachfolgendes Fenster **New Mail Configuration.**

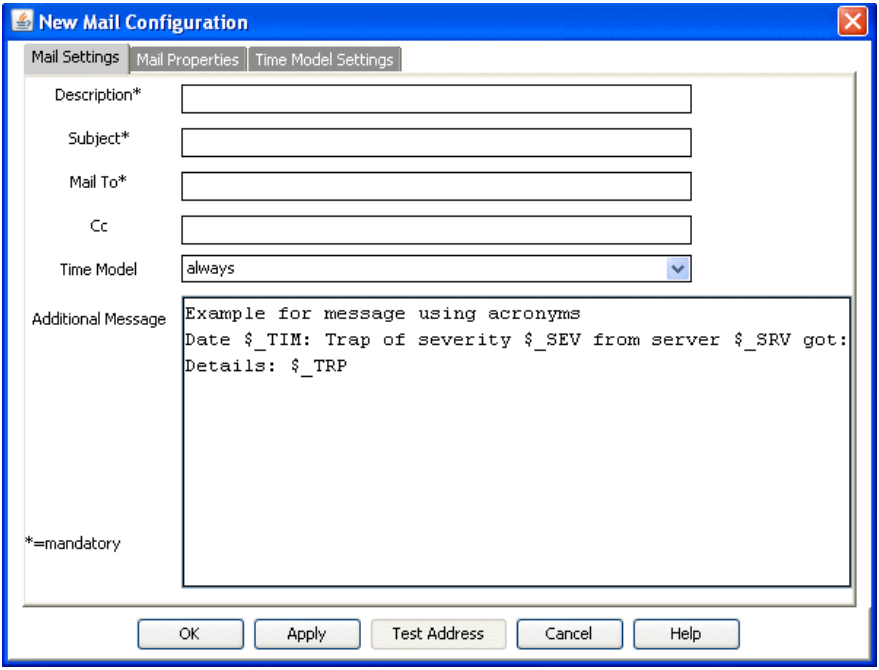


Bild 14: New Mail Configuration

In diesem Fenster können über die Registerkarten **Mail Settings, Mail Properties** und **Time Model Settings** alle zur Weiterleitung notwendigen Parameter definiert werden.Eingabefelder die mit * gekennzeichnet sind, müssen angegeben werden. Eine Angabe in den anderen Feldern ist optional.

Das Ergebnis der letzten Mail-Weiterleitung wird von ServerView Operations Manager in einer Log-Datei gespeichert.

Unter Windows befindet sich die Log-Datei "blat.txt" im Verzeichnis:

<install_path>\ServerView Services\scripts\ServerView\SnmpTrap

Unter Linux befindet sich die Log-Datei "smtpm.log" im Verzeichnis:

/opt/fujitsu/ServerViewSuite/web/cgi-bin/ServerView/SnmpTrap

Registerkarte **Mail Settings**

Die Registerkarte **Mail Settings** bietet Felder für die Mail-Einstellungen, von welchen zum Teil schon vordefinierte Mail-Einstellungen enthalten sind.

Die Eingabefelder im Fenster **Mail Settings** haben folgende Bedeutung:

Name	Bedeutung
Beschreibung	Name für die Mail-Einstellungen Wollen Sie bei einer bestehenden Mail-Weiterleitung die Mail-Einstellungen verändern (siehe Schaltfläche **Edit** Abschnitt "Alarme weiterleiten" auf Seite 54), ist dieses Feld mit dem bereits vergebenen Namen ausgefüllt und nicht aktiv.
Betreff	Betreff der Nachricht Der Betreff der Nachricht kann Makros enthalten (siehe Abschnitt "Makros" auf Seite 85). Enthält der Betreff nichtdarstellbare Zeichen, werden diese durch darstellbare Zeichen (z.B. Hexcode) ersetzt.
Mail To	E-Mail-Adresse der Person, an die Sie den Alarm senden möchten. Mehrere Adressen müssen durch Semikolon oder Komma getrennt werden.
Cc	E-Mail-Adresse der Person, an die eine Kopie des Alarms gesendet wird (optional) Mehrere Adressen müssen durch Semikolon oder Komma getrennt werden. Die Einstellung von zwei oder mehr Adressen ist nur möglich, wenn der Event Manager in einer Windows Umgebung ausgeführt wird.
Time Model	Zeitmodell, das festlegt, wann ein Alarm weitergeleitet werden soll Aus der Auswahlliste können Sie ein vordefiniertes Zeitmodell auswählen. Ein eigenes Zeitmodell können Sie über die Registerkarte **Time Model Settings** einstellen.

Tabelle 6: Eingabefelder im Fenster Mail Settings

Name	Bedeutung
Additional Message	Textfeld zum Definieren der Alarmmeldung. Über unterschiedliche Makros können Informationen der Server eingefügt werden (siehe Abschnitt "Makros" auf Seite 85). Zur einfacheren Handhabung wird hier schon ein Vorschlag vorgegeben. Löschen oder verändern Sie ihn gegebenenfalls.

Tabelle 6: Eingabefelder im Fenster Mail Settings

Registerkarte **Mail Properties**

Die Registerkarte **Mail Properties** bietet Felder für den Mail Server. Der Mail Server ist ein SMTP-Server.

Bei der Alarmweiterleitung ab ServerView V6.20 wird das MAPI nicht mehr unterstützt. Es werden nur noch SMTP-Server benutzt. Wird bei einem Upgrade der Mail-Dienst über das MAPI angesprochen, wird eine Warnung ausgegeben. Während des Setups werden alle MAPI-Ziele auf SMTP geändert. Die Einstellungen für den SMTP-Server müssen anschließend in der Komponente **Alarm Configuration** konfiguriert werden.

Die Eingabefelder im Fenster **Mail Properties** haben folgende Bedeutung:

Name	**Bedeutung**
Absender	Absender (SMTP)
Server	SMTP Server (SMTP)
User (optional)	Benutzername (SMTP)
Password (optional)	Identifizierung des Mailing-Systems (optional bei SMTP)
Bestätigen Sie das Passwort (optional)	Bestätigen Sie das Passwort (optional bei SMTP)
Port	Portnummer (SMTP) Standardwert ist **Port 25**

Tabelle 7: Eingabefelder im Fenster Mail Properties

Registerkarte **Time Model Settings**

Die Registerkarte **Time Model Settings** erlaubt es, ein Zeitmodell auszuwählen, hinzuzufügen oder zu ändern. Sie können stundenweise für die ganze Woche festlegen, wann ein Alarm weitergeleitet werden soll.

Wenn Sie auf die Schaltfläche **Test Address** klicken, wird eine Test-Mail versendet, um Ihre Einstellungen zu überprüfen.
Wenn Sie auf die Schaltfläche **OK** klicken, werden Ihre Einstellungen gespeichert und Sie kehren zum vorhergehenden Fenster zurück.
Je nach der Art der Weiterleitung und ausgewählter Registerkarte werden weitere Schaltflächen angeboten (siehe "Schaltflächen" auf Seite 40).

Virenscanner McAfee

Beim Virenscanner McAfee gibt es die Einstellung, die Programme daran hindert, E-Mails zu verschicken, wenn sie nicht registriert sind.

Um die Mail-Versender zu registrieren, muss der entsprechende Programmname eingetragen werden: Unter Windows **blat.exe,** unter Linux **smtpm**.

4.5 Mail- und Execute-Weiterleitung an Service Provider

Der Event Manager bietet die Möglichkeit, Alarme automatisch per Mail an den Service Provider weiterzuleiten.

Ist die Mail-Weiterleitung an den Service Provider aktiviert, wird dieser immer dann per E-Mail informiert, wenn bestimmte Traps auftreten. Die Gruppe der Traps, die eine Mail auslösen, wird vom Service Provider festgelegt und kann nur durch ihn verändert werden.

Das Ergebnis der letzten Mail-Weiterleitung wird von ServerView Operations Manager in einer Log-Datei gespeichert.

Unter Windows befindet sich die Log-Datei "blat.txt" im Verzeichnis:

<install_path>\ServerView Services\scripts\ServerView\SnmpTrap

Unter Linux befindet sich die Log-Datei "smtpm.log" im Verzeichnis:

/opt/fujitsu/ServerViewSuite/web/cgi-bin/ServerView/SnmpTrap

Mail-Weiterleitung aktivieren

Die Mail-Weiterleitung an den Service Provider aktivieren Sie im Fenster **Alarm Rules – Assign Destinations**, indem Sie in diesem Fenster die Alarmgruppe **Automatic Service Mail** auswählen.
Wenn Sie auf die Schaltfläche **Edit** klicken, öffnet sich das Fenster **Edit Automatic Service Mail Configuration**.
In diesem Fenster können Sie über die Registerkarte **Mail Settings** die notwendigen Einstellungen für die Mail-Weiterleitung an den Service Provider vornehmen.

Die Eingabefelder im Fenster **Mail Settings** haben folgende Bedeutung:

Name	**Bedeutung**
Mail To	E-Mail-Adresse des Service Centers
Cc	E-Mail-Adresse, an die eine Kopie der Service-Mail gesendet wird (optional)
Identnumber	eindeutige ID-Nummer des Servers i Diese Nummer ist mit dem Service Provider zu vereinbaren.
Name	Name des Server-Administrators
Phone	Telefonnummer des Server-Administrators
E-mail Address (optional)	E-Mail-Adresse, die vom Service Center für Rückmeldungen benutzt werden soll (optional)
Country ID (optional)	zweistelliger ISO-Code für das Land (optional) (z.B. DE für Germany)
Customer ID (optional)	Kundencode (optional) Der Kundencode muss mit dem Provider vereinbart werden.

Tabelle 8: Eingabefelder im Fenster Service Mail Settings

Mit der Option **Enabled** können Sie diese Konfiguration aktivieren oder deaktivieren.

Die Registerkarte **Mail Properties** bietet Felder für den Mail Server. Der Mail Server ist ein SMTP-Server.

Bei der Alarmweiterleitung ab ServerView V6.20 wird das MAPI nicht mehr unterstützt. Es werden nur noch SMTP-Server benutzt. Wird bei einem Upgrade der Mail-Dienst über das MAPI angesprochen, wird eine Warnung ausgegeben. Während des Setups werden alle MAPI-Ziele auf SMTP geändert. Die Einstellungen für den SMTP-Server müssen anschließend in der Komponente **Alarm Configuration** konfiguriert werden.

Die Eingabefelder im Fenster **Mail Properties** haben folgende Bedeutung:

Name	**Bedeutung**
Absender	Absender (SMTP)
Server	SMTP Server (SMTP)
User (optional)	Benutzername (SMTP)
Password (optional)	Identifizierung des Mailing-Systems (optional bei SMTP)
Bestätigen Sie das Passwort (optional)	Bestätigen Sie das Passwort (optional bei SMTP)
Port	Portnummer (SMTP) Standardwert ist **Port 25**

Tabelle 9: Eingabefelder im Fenster Mail Properties

Die Registerkarte **Exec Settings** bietet Felder für die Execute-Einstellungen. Zum Teil sind schon vordefinierte Einstellungen enthalten.

Die Eingabefelder im Fenster **Exec Settings** haben folgende Bedeutung:

Name	Bedeutung
Beschreibung (optional)	Name für die Execute-Einstellungen Wollen Sie bei einer bestehenden Execute-Weiterleitung die Execute-Einstellungen verändern (siehe Schaltfläche **Edit** Abschnitt "Alarme weiterleiten" auf Seite 54), ist dieses Feld mit dem bereits vergebenen Namen ausgefüllt und nicht aktiv.
Command	Name der Anweisung, die ausgeführt werden soll Der Name kann zusammen mit Argumenten als Kommandozeile eingegeben werden. In diesen Argumenten können über unterschiedliche Makros Informationen der Server eingefügt werden (siehe Abschnitt "Makros" auf Seite 85).
Working Directory (optional)	Name des Arbeitsverzeichnisses, in dem **Command** steht
Time Model (optional)	Zeigt an, ob ein Alarm zum Aufruf dieser Anweisung führen soll. Über die Auswahlliste können Sie das Zeitmodell aktivieren oder deaktivieren. Ist das Zeitmodell aktiviert, führt ein Alarm immer zum Aufruf dieser Anweisung.

Tabelle 10: Eingabefelder im Fenster Exec Settings

Wenn Sie im Fenster **Service Mail Settings** auf die Schaltfläche **Test Address** klicken, wird eine Test-Mail an den Service Provider gesendet. Das Service Center antwortet per E-Mail automatisch auf eingehende Test-Mails. Dabei wird jene Adresse verwendet, die im Eingabefeld **E-mail** angegeben wurde.

Zwischen der Versendung von identischen Mails ist ein Mindestzeitraum von 600 Sekunden festgelegt. Damit wird sichergestellt, dass keine redundanten Nachrichten weitergesendet werden.

Im Alarm Monitor werden Traps, die eine Service-Mail angestoßen haben, folgendermaßen gekennzeichnet:

Dieses Icon kennzeichnet einen Trap, der über die Service-Mail-Funktion weitergeleitet wurde.

Dieses Icon kennzeichnet einen Trap, der sowohl über die normale Mail-Funktion als auch über die Service-Mail-Funktion weitergeleitet wurde.

4.6 Popup-Einstellungen vornehmen

Wenn Sie **Popup** für das Weiterleiten ausgewählt haben, erscheint das Fenster **New Popup Configuration**. In diesem Fenster können Sie über die Registerkarten **Popup Settings** und **Time Model Settings** alle zur Popup-Weiterleitung notwendigen Einstellungen vornehmen.

Popup-Meldungen werden nur auf dem Local Host angezeigt. Sie können nicht auf einem anderen Rechner angezeigt werden.

Registerkarte **Popup Settings**

Die Registerkarte **Popup Settings** bietet Felder für die Popup-Einstellungen, von welchen zum Teil schon vordefinierte Einstellungen enthalten sind.

Die Eingabefelder im Fenster **Popup Settings** haben folgende Bedeutung:

Name	Bedeutung
Beschreibung	Name für die Popup-Einstellungen Wollen Sie bei einer bestehenden Popup-Weiterleitung die Popup-Einstellungen verändern (siehe Schaltfläche **Edit** Abschnitt "Alarme weiterleiten" auf Seite 54), ist dieses Feld mit dem bereits vergebenen Namen ausgefüllt und nicht aktiv.
Time Model	Zeitmodell, wann ein Alarm zu einer Popup-Meldung führen soll Aus der Auswahlliste können Sie ein vordefiniertes Zeitmodell auswählen. Ein eigenes Zeitmodell können Sie über die Registerkarte **Time Model Settings** einstellen.
Additional Message (optional)	Textfeld zum Definieren der Meldung des Popup-Fensters Über unterschiedliche Makros können Informationen der Server eingefügt werden (siehe Abschnitt "Makros" auf Seite 85). Ab Windows Server 2008 wird bei der Ausgabe nach 255 Zeichen abgeschnitten.

Tabelle 11: Eingabefelder im Fenster Popup Settings

Registerkarte **Time Model Settings**

Die Registerkarte **Time Model Settings** erlaubt es, ein Zeitmodell auszuwählen, hinzuzufügen oder zu ändern. Sie können stundenweise für die ganze Woche festlegen, wann ein Alarm weitergeleitet werden soll.

Hinweise für Linux

1. Um die weitergeleiteten Alarmmeldungen zu empfangen, muss ein Anwender an der Linux System-Konsole angemeldet sein. Ist kein Anwender an der Linux System-Konsole angemeldet, werden die weitergeleiteten Alarmmeldungen nicht gespeichert. Sie werden somit nicht beim nächsten Login an der System-Konsole ausgegeben.

2. Da bei Linux-Systemen der Anwender an einer virtuellen System-Konsole angemeldet ist, kann er entweder grafische Oberflächen (GUI-Session z.B. Gnome oder KDE) oder die Kommandoschnittstelle (CLI-Session) benutzen. Abhängig von der gewählten virtuellen System-Konsole ist die Darstellung des Layouts.

   Bei einer CLI-Session erhält der angemeldete Anwender die weitergeleitete Alarmmeldung als Klartext-Meldung.

   Bei einer GUI-Session wird die weitergeleitete Alarmmeldung in einem (nicht modalen) Popup-Fenster ausgegeben.

3. Der Weiterleitungs-Service benutzt die Datenbank unter /var/run/utmp, um Informationen über die an der System-Konsole angeschlossenen Anwender zu erhalten. Die Einträge in der Datenbank sollten deshalb korrekt sein.
   Wird eine Grafik-Session an der System-Konsole mit dem Programm **startx** gestartet, werden unter /var/run/utmp nicht die notwendigen Einträge gemacht. Die weitergeleiteten Alarme werden dann nicht ausgegeben.
   Um die weitergeleiteten Alarmmeldungen an der ServerView Management Station als Popup-Meldungen zu empfangen, sollte das Linux Betriebssystem nach einem Systemstart im Grafik-Modus (Runlevel5) beginnen.
   Der Weiterleitungs-Service leitet Alarme nicht an Xconsolen weiter.

4.7 Pager-Einstellungen vornehmen (COM Port & Modem)

Wenn Sie **Pager** für das Weiterleiten ausgewählt haben, erscheint das Fenster **New Pager Configuration.** In diesem Fenster können Sie über die Registerkarten **Pager Settings** und **Modem Settings** die unterschiedlichen Einstellungen für die seriellen Schnittstellen und die daran angeschlossenen Modems (Pager-Typen) vornehmen.

Folgende Werte können Sie festlegen:

– den Namen der verfügbaren Schnittstellen (z.B. COM2 oder COM4)
– die maximale Übertragungsgeschwindigkeit (Baud rate)
– die Art der Datenflusskontrolle
– die Initialisierungs- und Reset-Zeichenkette für das Modem

Die Eingabefelder im Fenster **New Pager Configuration** haben folgende Bedeutung:

Name	**Bedeutung**
Beschreibung	Name für die Pager-Einstellungen
Owner	Name des Eigentümers
Com Port	Name der seriellen Schnittstellen. Die Auswahlliste enthält die Namen der verfügbaren Schnittstellen. Sie können eine spezielle Schnittstelle oder den Eintrag **Any Available** auswählen. Bei Any Available kann jede verfügbare Schnittstelle mit Ihren COM Ports verbunden werden. Das ist sinnvoll bei häufigem Wechsel der verbundenen Geräte.

Tabelle 12: Eingabefelder im Fenster Mail Settings

Name	Bedeutung
Pager Number	(Telefon-)Nummer des Pagers Bei einer SMS kann es sein, dass der Zielnummmer ein zusätzliches Präfix des entsprechenden Service-Dienstes vorangestellt werden muss. zum Beispiel: D1-Service in Deutschland: 49171XXXXXXX (XXXXXXX = Pager ID) 49171 muss vorangestellt werden (ohne 00) D2-Service in Deutschland: 0049172XXXXXXX 0049172 ist optional
Time Model	Zeitmodell, das festlegt, wann ein Alarm weitergeleitet werden soll Aus der Auswahlliste können Sie ein vordefiniertes Zeitmodell auswählen. Ein eigenes Zeitmodell können Sie über die Registerkarte **Time Model Settings** einstellen.
Retry Delay	Verzögerungszeit in Minuten zwischen zwei Pager-Versuchen Wählen Sie die Zeit nicht zu kurz, da Aufrufe an einen Pager durch den Service-Provider um einige Minuten verzögert werden können. Beachten Sie auch die Zeit, die benötigt wird, um die Management-Station zu erreichen. Diese Verzögerungszeit kann etwa fünf oder mehr Minuten umfassen.
Retries	Anzahl der Versuche, die unternommen werden sollen, einen Alarm an einen Pager weiterzuleiten, bevor eine Meldung erscheint.
Pager Type	Art des Pagers (signal/numeric/alpha/SMS1-Service/ SMS2-Service/NTT-Service) Wählen Sie die falsche Pager-Art, wird die Übertragung aufgrund eines ungültigen Kommunikationsprotokolls ignoriert.

Tabelle 12: Eingabefelder im Fenster Mail Settings

Über die Registerkarten **Pager, SMS-1** oder **SMS-2** legen Sie den Pager-Dienst fest.

Die Registerkarte **Server Num** informiert darüber, welche Server-Nummern welchem Server-Namen zugeordnet sind. Die Server-Nummer wird an den Pager-Typ **numeric** gesendet.

Wenn Sie auf die Schaltfläche **Test** klicken, können Sie Ihre Einstellungen überprüfen.

Für jede Service-Nummer machen Sie Einstellungen für Datenbits, Parität und Stopbits und Sie definieren den Prompt, den der Pager-Dienst bei Meldungen verwendet.
Mit SMS1- und SMS2-Service können zwei Dienste mit unterschiedlichen Protokollen in Anspruch genommen werden, um ein GSM-Handy anzusprechen. SMS1 verwendet das TAP-Protokoll, SMS2 verwendet das UDP-Protokoll.

Baud Rate	2400 bps, 1200 bps oder 300 bps
Data bits	8
Parity	none
Stop-Bits	1
Dial-Prefix	ATDP0,01691

Tabelle 13: Beispiel-Einstellungen für „Cityruf“ der Deutschen Telekom

Wenn Sie die Einstellungen für die seriellen Schnittstellen festgelegt haben, dann können Sie festlegen, ob ein Alarm einen Anruf auf einem Pager oder Handy auslösen soll (siehe hierzu auch Abschnitt "Alarme weiterleiten" auf Seite 54).

4.8 Execute-Einstellungen vornehmen

Wenn Sie **Execute** für das Weiterleiten ausgewählt haben, erscheint das Fenster **New Execute Configuration**. In diesem Fenster können Sie über die Registerkarten **Exec Settings** und **Time Model Settings** alle zur Execute-Weiterleitung notwendigen Einstellungen vornehmen.

Registerkarte **Exec Settings**

Die Registerkarte **Exec Settings** bietet Felder für die Execute-Einstellungen, von welchen zumTeil schon vordefinierte Einstellungen enthalten sind.

Die Eingabefelder im Fenster **Exec Settings** haben folgende Bedeutung:

Name	Bedeutung
Beschreibung	Name für die Execute-Einstellungen Wollen Sie bei einer bestehenden Execute-Weiterleitung die Execute-Einstellungen verändern (siehe Schaltfläche **Edit** Abschnitt "Alarme weiterleiten" auf Seite 54), ist dieses Feld mit dem bereits vergebenen Namen ausgefüllt und nicht aktiv.
Command	Name der Anweisung, die ausgeführt werden soll Der Name kann zusammen mit Argumenten als Kommandozeile eingegeben werden. In diesen Argumenten können über unterschiedliche Makros Informationen der Server eingefügt werden (siehe Abschnitt "Makros" auf Seite 85).
Working Directory (optional)	Name des Arbeitsverzeichnisses, in dem **Command** steht
Time Model	Zeitmodell, wann ein Alarm zum Aufruf dieser Anweisung führen soll Aus der Auswahlliste können Sie ein vordefiniertes Zeitmodell auswählen. Ein eigenes Zeitmodell können Sie über die Registerkarte **Time Model Settings** einstellen.

Tabelle 14: Eingabefelder im Fenster Exec Settings

Registerkarte **Time Model Settings**

Die Registerkarte **Time Model Settings** erlaubt es, ein Zeitmodell auszuwählen, hinzuzufügen oder zu ändern. Sie können stundenweise für die ganze Woche festlegen, wann ein Alarm weitergeleitet werden soll.

Für Windows Server 2008 ist das CUI-Kommando das einzige Kommando, das für die Ausführung des Programms benutzt werden kann.

4.9 Broadcast-Einstellungen vornehmen

Broadcast ist eine Übertragungsart bei der gleichzeitig an mehreren Servern oder Servergruppen ein Popup-Fenster oder eine Meldung angezeigt wird.Wenn Sie Broadcast für das Weiterleiten ausgewählt haben, erscheint das Fenster **New Broadcast Configuration**. In diesem Fenster können Sie über die Registerkarten **Broadcast Settings** und **Time Model Settings** alle zur Broadcast-Weiterleitung notwendigen Einstellungen vornehmen.

Registerkarte **Broadcast Settings**

Die Registerkarte **Broadcast Settings** bietet Felder für die Broadcast-Einstellungen, von welchen zum Teil sind schon vordefinierte Einstellungen enthalten sind.

Die Eingabefelder im Fenster **Broadcast Settings** haben folgende Bedeutung:

Name	Bedeutung
Beschreibung	Name für die Broadcast-Einstellungen Wollen Sie bei einer bestehenden Broadcast-Weiterleitung die Broadcast-Einstellungen verändern (siehe Schaltfläche **Edit** Abschnitt "Alarme weiterleiten" auf Seite 54), ist dieses Feld mit dem bereits vergebenen Namen ausgefüllt und nicht aktiv.

Tabelle 15: Eingabefelder im Fenster Broadcast Settings

Name	Bedeutung
Time Model	Zeitmodell, das festlegt, wann ein Alarm weitergeleitet werden soll Aus der Auswahlliste können Sie ein vordefiniertes Zeitmodell auswählen. Ein eigenes Zeitmodell können Sie über die Registerkarte **Time Model Settings** einstellen.
Mode Special user All users of domain All users with session	Festlegung des Modus für die Broadcast-Weiterleitung Nur ein Anwender wird informiert. Der Name muss im Eingabefeld eingetragen werden. Alle Anwender werden informiert, die zur gleichen Domäne der Weiterleitung gehören. (gültig nur bei Windows, Standard) Ab Windows Server 2008 wird domain nicht mehr unterstützt. Alle Anwender werden informiert, die durch eine beliebige Session mit der Weiterleitung verbunden sind. (Standard bei Linux)
Additional Message (optional)	Textfeld zum Definieren der Meldung des Broadcast-Fensters Über unterschiedliche Makros können Informationen der Server eingefügt werden (siehe Abschnitt "Makros" auf Seite 85). Ab Windows Server 2008 wird bei der Ausgabe nach 255 Zeichen abgeschnitten.

Tabelle 15: Eingabefelder im Fenster Broadcast Settings

Registerkarte **Time Model Settings**

Die Registerkarte **Time Model Settings** erlaubt es, ein Zeitmodell auszuwählen, hinzuzufügen oder zu ändern. Sie können stundenweise für die ganze Woche festlegen, wann ein Alarm weitergeleitet werden soll.

Hinweise für Linux

Der Weiterleitungs-Service benutzt die Datenbank unter /var/run/utmp (utmp(5)), um Informationen über die angeschlossenen Anwender und über die Art der Session (GUI oder CLI) zu erhalten. Alle Sessions (lokal oder remote) sollten deshalb korrekt in der utmp-Datenbank registriert sein.

Die KDE-Session macht bei SuSE-Linux und RedHat-Linux keine utmp-Einträge über die Konsole oder die Emulation, die mit ihr gestartet wird. Weitergeleitete Alarmmeldungen werden deshalb nicht in diesen Fenstern ausgegeben.

Diese Einschränkungen gelten nicht für die GNOME-Sessions mit SuSE-Linux und RedHat-Linux, sowie für KDE-Sessions mit Caldera OpenLinux.

Hinweise für Windows

Wegen Störungen des benutzten Windows Messenger-Services kann eine Weiterleitung mit Broadcast fehlschlagen. Mit dem Kommando net send können Sie das überprüfen.

4.10 Trap-Einstellungen vornehmen

Wenn Sie **Station** für das Weiterleiten ausgewählt haben, erscheint das Fenster **New Station Configuration**. In diesem Fenster können Sie über die Registerkarten **Station Settings** und **Time Model Settings** alle zur Trap-Weiterleitung notwendigen Einstellungen vornehmen.

Registerkarte **Station Settings**

Die Registerkarte **Station Settings** bietet Felder für die Trap-Einstellungen, von welchen zum Teil schon vordefinierte Einstellungen enthalten sind.

Die Eingabefelder im Fenster **Station Settings** haben folgende Bedeutung:

Name	Bedeutung
Station Name	Name der Station, an die die Traps weitergeleitet werden Wollen Sie bei einer bestehenden Trap-Weiterleitung die Trap-Einstellungen verändern (siehe Schaltfläche **Edit** Abschnitt "Alarme weiterleiten" auf Seite 54), ist dieses Feld mit dem bereits vergebenen Namen ausgefüllt und nicht aktiv.
Community	Name der Community, an die weitergeleitet werden soll Standardwert ist **public**
Time Model	Zeitmodell, das festlegt, wann ein Alarm weitergeleitet werden soll Aus der Auswahlliste können Sie ein vordefiniertes Zeitmodell auswählen. Ein eigenes Zeitmodell können Sie über die Registerkarte **Time Model Settings** einstellen.
IP Address	Internetprotokolladresse

Tabelle 16: Eingabefelder im Fenster Station Settings

Name	Bedeutung
Forwarding Mode	Festlegung des Modus für die Weiterleitung.
Normal	Dieser Modus wertet den Alarm aus und leitet ihn an die Management-Station weiter.
Pass Through	Diesen Modus gibt es in einer ursprünglichen Variante und in der Variante Transparent. Die ursprüngliche Variante reicht den Alarm direkt an die Management-Station durch. Der Alarm erscheint dort so, als ob er direkt vom Server kommt. In diesem Modus wird der Trap nur einmal weitergeleitet.
Transparent	Die Variante **Transparent** leitet den Trap genauso an die Management-Station weiter, wie er empfangen wurde. Es ist nicht möglich zu entscheiden, ob der Trap vom Agenten gesendet wurde oder vom Event Manager weitergeleitet wurde.

Tabelle 16: Eingabefelder im Fenster Station Settings

Registerkarte **Time Model Settings**

Die Registerkarte **Time Model Settings** erlaubt es, ein Zeitmodell auszuwählen, hinzuzufügen oder zu ändern. Sie können stundenweise für die ganze Woche festlegen, wann ein Alarm weitergeleitet werden soll.

4.11 Makros

Im Folgenden finden Sie eine Liste von Makros, die bei der Weiterleitung von Alarmen (z.B. Mail, Pager) benutzt werden können.

Diese Makros werden durch die entsprechenden Informationen der Server ersetzt, die den Alarm melden.

Name	Bedeutung
$_SRV	Name des Servers
$_TRP	Text der Alarmmeldung
$_TYP	Kurzbeschreibung des Alarms
$_IPA	IP-Adresse des Servers
$_CTY	Community
$_SEV	Fehlergewichtung des Alarms (critical, major, minor, informational, unknown)
$_TIM	Zeitmodell (Format : yyyy-mm-dd-hh.mm.ss) Lokaler Zeitplan der Management-Station, nach dem ein Alarm weitergeleitet wird.
$_IDN	Ident-Nummer des Servers
$_OMS	Name der Management-Station
$_MIB	Name der MIB-Datei mit dem erhaltenen Alarm
$_SPC	Spezifische Nummer des erhaltenen Alarms
$_MDL	Fujitsu REMCS ID der Hardware, die den Alarm meldet

Tabelle 17: Makros

4.12 Beispiel einer Alarmkonfiguration

Dieser Abschnitt enthält ein typisches Beispiel für eine Alarmkoniguration.

Ziel

Wenn an dem Server **ALARMTEST** ein Ereignis mit der Alarmstufe critical auftritt, wird eine Mail an den Administrator gesendet (**admin@test.co.jp**).

Voraussetzungen

- Der ServerView-Agent läuft auf dem verwalteten Server, und der Server ist als Management-Ziel im ServerView Operations Manager in dem selben Netzwerk registriert.
- Test-Traps von dem ServerView-Agent zum ServerView Operations Manager funktionieren normal.
- Der ServerView Operations Manager kann auf den SMTP Server (111.222.3.20) zugreifen, während er in Betrieb ist.

Konfigurationsvorgang

► Führen Sie einen der beiden folgenden Operationen durch:

- Wenn Sie von dem Startfenster des ServerView Operations Managers ausgehen:

  Klicken Sie auf **Alarm Configuration**.

- Wenn Sie von einem Fenster einer ServerView-Komponente ausgegehen:

  Klicken Sie auf **Event Management – Alarm Configuration** in der Menüzeile am oberen Rand des Fensters.

Das Fenster **Manage Alarm Rules** öffnet.

► Klicken Sie auf **Add**.

Der Dialog **New Name** wird geöffnet.

► Geben Sie z.B. **CriticalMail** in dem Dialogfenster **New Name** und klicken Sie auf **OK**.

► Klicken Sie auf **Apply** und dann auf **Next**.Das Fesnter **Assign Servers** öffnet.

- ► Wählen Sie den Server **ALARMTEST** in der Serverliste und klicken auf die Schaltfläche >.
- ► Klicken Sie auf **Apply** und dann auf **Next**.Das Fenster **Assign Alarms - Individual Alarms** öffnet.
- ► Klicken Sie erneut auf **Next**.

  Das Fenster **Assign Alarms - Type of Alarms** öffnet.
- ► Wählen Sie **All alarms of severity critical**.
- ► Klicken Sie auf **Apply** und dann auf **Next**.

  Das Fenster **Assign Destinations** öffnet.
- ► Klicken Sie auf **Add**.

  Das Dialogfenster **Type of new Destination** öffnet.
- ► Wählen Sie **Mail** und klicken Sie auf **OK**.

  Das Fenster **New Mail Configuration** öffnet.
- ► Geben Sie auf der Registerkarte **Mail Settings** in jedem Feld die erforderlichen Angaben ein.

  Beschreibung
  In diesem Beispiel: **MailSet** als Zielname

  Betreff
  In diesem Beispiel: **Critical Error occurred**

  Mail to
  In diesem Beispiel: **admin@test.co.jp** als Administrator

  Time Model
  In diesem Beispiel: **always**

  Absender
  In diesem Beispiel: **ALARMTEST**

  Server
  In diesem Beispiel: **111.222.3.20**

  Konfiguriert die Einstellungen für Mails an den Administrator (**admin@test.co.jp**) von dem Server **ALARMTEST**.

- ► Klicken Sie auf **Apply** und dann auf **Next**.
- ► Sobald die Test-Mail erfolgreich versendet wurde, klicken Sie **OK**. Damit kehren Sie zurück in das Fenster **Assign Destinations**.
- ► Wählen Sie das neuangelegte **MailSet** und klicken Sie auf die Schaltfläche >.
- ► Klicken Sie auf **Apply**.

5 Traps

Treten bei einer Netzkomponente besondere Ereignisse auf, so kann der SNMP-Agent die Nachricht darüber an einen oder mehrere Manager senden, um diese von dem Ereignis zu unterrichten. Eine solche Nachricht wird in SNMP als Trap bezeichnet. Der Manager kann auf der Basis des eintreffenden Traps auf Ereignisse im Netz reagieren. Eine Trap-Nachricht kann über die Trap-ID und die MIB-OID eindeutig identifiziert werden.

In WBEM (Web-Based Enterprise Management) Umgebungen senden CIM Provider die Ereignisse als CIM Indications. CIM Indications entsprechen im Wesentlichen den Traps, die in der SC2.MIB definiert sind. Abhängig von den CIM Providern, die in einer Management-Umgebung installiert sind, kann es jedoch einige in der SC2.MIB definierte Ereignisse (Traps) geben, für die keine entsprechenden Indications gesendet werden.

5.1 Trap-Information abfragen

Im Hilfe-System vom Event Manager erhalten Sie ausführliche Informationen zu den vom Event Manager standardmäßig unterstützten MIBs und deren Traps.

Sie erhalten das entsprechende Übersichtsfenster entweder über das Startfenster des Event Managers oder über das Fenster **Alarm Monitor**.

– Trap-Informationen über das Startfenster des Event Managers

  ► Starten Sie den Event Manager.

  ► Wählen Sie unter **Help** den Eintrag **On Suite**.

  ► Wählen Sie dann unter **Event Management** den Eintrag **Alarm Monitor**.

  ► Klicken Sie in dem angezeigten Fenster auf den Link **Event Manager**.

  ► Wählen Sie unter **Alarms** den Eintrag **Agent Alarm Information**.

– Trap-Informationen über Fenster **Alarm Monitor**

  ► Starten Sie den Event Manager.

  ► Wählen Sie unter **Event Management** den Eintrag **Alarm Monitor**.

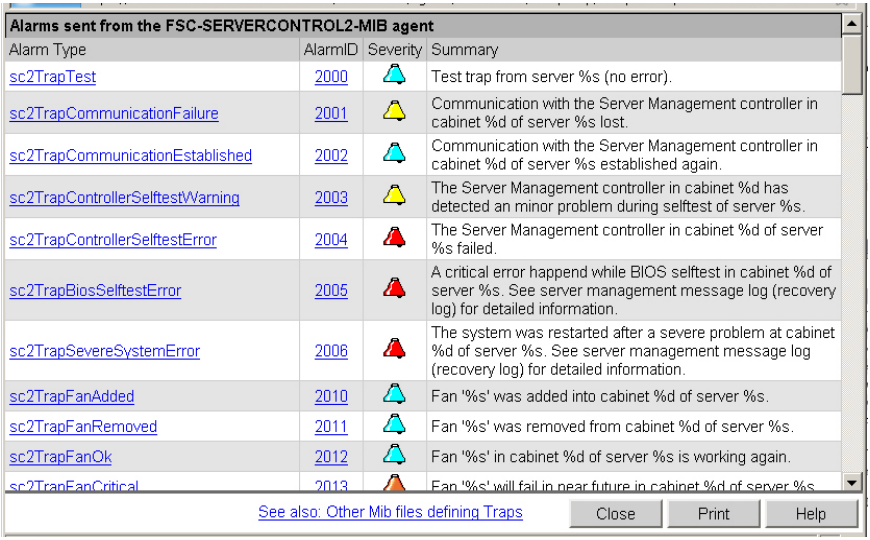
- ► Wählen Sie im Fenster **Alarm Monitor** in der Menüleiste den Eintrag **Help – On Alarm Monitor**.
- ► Klicken Sie in dem angezeigten Fenster auf den Link **Event Manager**.
- ► Wählen Sie unter **Alarms** den Eintrag **Agent Alarm Information**.

Die Trap-Informationen können analog auch über das Startfenster des ServerView Operations Managers abgerufen werden.

Das Fenster **Alarm Mibs** wird angezeigt.

Bild 15: MIB-Übersicht im Event Manager - Beispiel

Wenn Sie eine MIB ausgewählt haben, erhalten Sie ein Fenster mit detaillierten Informationen zu den Traps, z.B.:



Alarms sent from the FSC-SERVERCONTROL2-MIB agent

Alarm Type	AlarmID	Severity	Summary
sc2TrapTest	2000		Test trap from server %s (no error).
sc2TrapCommunicationFailure	2001		Communication with the Server Management controller in cabinet %d of server %s lost.
sc2TrapCommunicationEstablished	2002		Communication with the Server Management controller in cabinet %d of server %s established again.
sc2TrapControllerSelftestWarning	2003		The Server Management controller in cabinet %d has detected an minor problem during selftest of server %s.
sc2TrapControllerSelftestError	2004		The Server Management controller in cabinet %d of server %s failed.
sc2TrapBiosSelftestError	2005		A critical error happend while BIOS selftest in cabinet %d of server %s. See server management message log (recovery log) for detailed information.
sc2TrapSevereSystemError	2006		The system was restarted after a severe problem at cabinet %d of server %s. See server management message log (recovery log) for detailed information.
sc2TrapFanAdded	2010		Fan '%s' was added into cabinet %d of server %s.
sc2TrapFanRemoved	2011		Fan '%s' was removed from cabinet %d of server %s.
sc2TrapFanOk	2012		Fan '%s' in cabinet %d of server %s is working again.
sc2TrapFanCritical	2013		Fan '%s' will fail in near future in cabinet %d of server %s

See also: Other Mib files defining Traps | Close | Print | Help

Bild 16: Detailinformation zu Traps aus einer MIB (Beispiel)

Über die Schaltfläche **Print** in diesem Fenster können Sie sich diese Information auch ausdrucken.

5.2 Traps im Windows Event-Log anzeigen

Bei der Installation der Windows-Agenten können Sie angeben, ob die Traps aus den Fujitsu MIBs (z.B. HD.MIB, Mylex.MIB) auch in das Windows Event-Log geschrieben werden sollen. Die Trap-ID dieser MIBs werden im Event-Log um 10000 erhöht angezeigt und nicht wie in den nachfolgenden Trap-Beschreibungen (z.B. wird der Trap **mylexBBUFound** mit der Trapnummer 275 im Event-Log mit der Trapnummer 10275 angezeigt).

Mit dem Event Manager können Sie über die Alarmweiterleitung (**Logging**) festlegen, dass Traps in die Windows- bzw. in die Linux Event-Log geschrieben werden. Der Quellname der Ereignisse in der Event-Log ist sowohl in Linux wie auch in Windows **ServerView Services**.

Der Event-Typ von **UnknownTrap** in der Event-Log wird auf **Information-**Level gesetzt.

5.3 Trapübersicht

Die folgende Tabelle gibt einen Überblick über die MIBs, die im Event Manager integriert sind. Diese Inhalte werden häufig aktualisiert. Deshalb stellt diese Tabelle und auch die nachfolgenden Traplisten nur eine Momentaufnahme dar und erhebt keinen Anspruch auf Vollständigkeit. Welche MIBs aktuell im Event Manager integriert sind, erfahren Sie über das Fenster **Alarm Configuration** (in der Spalte **MIB** in dem Dialogfenster **Alarm Rules - Assign Alarms**) oder über die Online-Hilfe des Event Managers.

In den anschließenden Abschnitten finden Sie eine Übersicht über die wichtigsten Traps. In nachfolgenden Abschnitten dieses Kapitels sind die Traps alphabetisch nach Kategorie sortiert. Innerhalb jeder Kategorie sind die Traps alphabetisch nach Name sortiert.

Unter der Spalte **Bemerkung** finden Sie die Information, welche Traplisten in den folgenden Abschnitten aufgelistet sind und auf welcher Seite sie zu finden sind. Sie haben auch die Möglichkeit, sich die Trapliste über den Event Manager auszudrucken. Weitere Informationen entnehmen Sie dem Abschnitt "Trap-Information abfragen" auf Seite 89.

MIB	Traps von	Bemerkung
aac.mib	Adaptec controller	
ADICLIBMIB-v2.mib		siehe Seite 130
adptinfo.mib		
Asmpro.mib	ASM PRIVATE COMMIB traps	siehe Seite 185
baspCfg.mib		
baspStat.mib		
baspTrap.mib	Broadcom Advanced Server-Traps	
BIOS.mib		
BUS.mib		
clariion1.mib	FibreCat	
clariion_fsc_2.mib	FibreCat	
Cmc32.mib	Rittal Rack-Überwachung	
CMS-TC.mib		
Ddm.mib	DuplexDataManager-Traps	siehe Seite 113
dec.mib	StorageWorks Enterprise Array Manager von Compaq	siehe Seite 137
desktrap.mib	DeskView-Traps	
dhtraps.mib		
domagt.mib		
dptscsi.mib	DPT-SCSI-Traps	siehe Seite 110
Duralink.mib	ADAPTEC Duralink-Traps	siehe Seite 98
DW.mib	DuplexWrite-Traps	siehe Seite 117
egeneraV1.mib		
Ether.mib		
eurologic.mib	FibreCat	
F5emt2o.mib	HP OpenView Network Node Manager	
fcswitch.mib	Fibre Channel Switch	
FSC-AC-MIBV1.mib		
FSC-KVMS3-TRAP.mib		
FSC-RCA4PLUS-TRAP.mib		

Tabelle 18: MIB-Übersicht

MIB	Traps von	Bemerkung
FSC-S21611-TRAP.mib		
Hd.mib	ServerView-Agent: Platten	siehe Seite 120
HPI-MIBV1.mib		
INTELLAN_V1.mib		
INVENT.mib		
iommib.mib	Adaptec	
Ldcm.mib	LAN Desk Client Manager von Intel Traps	siehe Seite 188
Ldsm.MIB	LAN Desk Server Manager von Intel Traps	siehe Seite 188
log3v1.mib	PRIMEPOWER Logbuch-Einträge	siehe Seite 131
Lsi1030.mib		
LSIRAID-IDE.mib		
Megaraid.mib	RAID-Adapter von American Mega Trends Inc.	siehe Seite 144
MIxraid.mib	MylexDiskArrayController-Traps	
MMB-COM-MIB.mib		
MMB-ComTrap-MIB.mib		
mp.mib	MultiPath-Traps	siehe Seite 122
Mylex.mib	RAID Controller (Mylex DAC 960)	siehe Seite 123
net-snmp.mib		
netapp.mib	Network-Appliance-Traps	
NT.mib		
NTCluster.MIB	Microsoft Cluster	siehe Seite 107
NW.mib		
OS2.mib		
pcihotplug.mib	SCSI-Geräte Hot Plug-Traps	siehe Seite 129
Powernet.mib	American-Power-Conversion-Traps	siehe Seite 98
Ppc.mib	USV-Traps 2	siehe Seite 197
primepower_xscf.mib	PRIMEPOWER Hardware Diagnose	siehe Seite 130
promiseraid.mib		
promisev1.mib	Promise-RAID-Controller-Traps	
PSA-COM-MIB.mib	PRIMEQUEST-Traps	

Tabelle 18: MIB-Übersicht

MIB	Traps von	Bemerkung
PSA-ComTrap-MIB.mib	PRIMEQUEST-Traps	
PSA-ExternalFileUnitTrap-MIB.mib	PRIMEQUEST-Traps	
PSA-LIN-MIB.mib	PRIMEQUEST-Traps	
PSA-LinBcm5700Trap-MIB.mib	PRIMEQUEST-Traps	
PSA-LinEmulexTrap-MIB.mib	PRIMEQUEST-Traps	
PSA-LinGdsTrap-MIB.mib	PRIMEQUEST-Traps	
PSA-LinGlsTrap-MIB.mib	PRIMEQUEST-Traps	
PSA-LinGrmpdTrap-MIB.mib	PRIMEQUEST-Traps	
PSA-LinIntelE1000Trap-MIB.mib	PRIMEQUEST-Traps	
PSA-LinIntelE100Trap-MIB.mib	PRIMEQUEST-Traps	
PSA-LinLanComTrap-MIB.mib	PRIMEQUEST-Traps	
PSA-LinLsiLogicTrap-MIB.mib	PRIMEQUEST-Traps	
PSA-LinScsiComTrap-MIB.mib	PRIMEQUEST-Traps	
PSA-LinTg3Trap-MIB.mib	PRIMEQUEST-Traps	
PSA-WIN-MIB.mib	PRIMEQUEST-Traps	
PSA-WinBcm5700Trap-MIB.mib	PRIMEQUEST-Traps	

Tabelle 18: MIB-Übersicht

MIB	Traps von	Bemerkung
PSA-WinEmulexTrap-MIB.mib	PRIMEQUEST-Traps	
PSA-WinIntelE1000Trap-MIB.mib	PRIMEQUEST-Traps	
PSA-WinIntelE100Trap-MIB.mib	PRIMEQUEST-Traps	
PSA-WinLsiLogicTrap-MIB.mib	PRIMEQUEST-Traps	
RAID.mib		
RFC1157.mib		
RFC1213.mib		
RFC1285.mib		
RFC1628.mib		
RMS-C_SNMPv1_contact.mib		
RMS-C_SNMPv1_humid1.mib		
RMS-C_SNMPv1_humid2.mib		
RMS-C_SNMPv1_main.mib		
RMS-C_SNMPv1_output.mib		
RMS-C_SNMPv1_temp2.mib		
Rompilot.mib	RomPilot-Traps	see Seite 147
S31.mib	Blade-Server-Traps	
SANMgrV1.mib	Pathlight SAN Data Gateway	

Tabelle 18: MIB-Übersicht

MIB	Traps von	Bemerkung
SC.mib	ServerControl-Traps	see Seite 149
SC2.mib		
SECURITY.mib		
Servervi.mib	FUJITSU-ServerVisor-Traps	
ServerView.mib	ServerView-Traps	see Seite 163
Status.mib	ServerView-Status-Traps	see Seite 164
tapealrt.mib	Bandlaufwerke-Traps	see Seite 165
Threshold.mib		
TOK.mib		
Trap.mib	ServerView-Traps	see Seite 189
trap1493.mib	Switch-Traps	
trap1757.mib	Switch-Traps	
unicorn-trap.mib		
uniserv.mib	PRIMEPOWER Enterprise Server	see Seite 132
UNIX.mib		
Upsman.mib	Enterprise Specific Top Level MIB by Quazar GmbH, USV-Traps 1	see Seite 196
v1_fscHaCI.mib	PRIMECLUSTER-Traps	
VMWARE-TRAPS-MIB.mib		
VV.mib		
WFM.mib	WfM-Traps (Wired for Management)	
wsatrap.mib	PRIMEPOWER hardware	

Tabelle 18: MIB-Übersicht

5.3.1 Adaptec-Traps (Duralink.mib)

MIB-OID: 1.3.6.1.4.1.795.3.1.2.3

Im Folgenden finden Sie eine alphabetische Übersicht über die Adaptec-Traps.

Trap-Name	ID	Bedeutung	Fehlerklasse
duralinkStatusTrap	1	Der Status des Anschlusses hat sich geändert.	informational

Tabelle 19: Adaptec-Traps

5.3.2 APC-Traps (Powernet.mib)

MIB-OID: 1.3.6.1.4.1.318

Im Folgenden finden Sie eine alphabetische Übersicht über die APC-Traps.

Trap-Name	ID	Bedeutung	Fehlerklasse
baseFanFailure	25	Die Überbrückungsstromversorgung des Basismoduls ist defekt.	major
batteryPackComm Established	27	Die unterbrechungsfreie Stromversorgung (USV) steht in Verbindung mit dem externen Batteriesatz.	informational
batteryPackCommLost	26	Verbindung zu externen Batteriesätzen unterbrochen.	major
bypassPowerSupply Failure	24	Die Überbrückungsstromversorgung des Basismoduls ist defekt.	major
calibrationStart	28	Von der USV wurde ein Test zur Feststellung der Batterieladestärke eingeleitet.	informational

Tabelle 20: APC-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
codeAuthentication Done	32	Die Authentifizierung auf Grundlage des Agent-Codeabbilds wurde durchgeführt.	informational
communication Established	8	Verbindung zwischen Agent und Stromversorgung hergestellt.	informational
communicationLost	1	Verbindung zwischen Agent und Stromversorgung unterbrochen.	major
contactFault	18	Einer der Kontakte an der Measure-UPS ist von seiner Standardposition abgewichen.	major
contactFaultResolved	19	Ein Fehler an einem der Measure-UPS-Kontakte wurde beseitigt.	informational
hardwareFailure Bypass	20	Die unterbrechungsfreie Stromversorgung erfolgt auf Grund eines Hardwarefehlers über eine Überbrückung.	major
lowBattery	7	Die Ladung der Systembatterien der USV ist nahezu erschöpft. Wenn die Stromversorgung nicht wiederhergestellt wird, setzt sich die USV selbst in den Modus **sleep** und unterbricht umgehend die Stromversorgung.	major
powerRestored	9	Die Stromversorgung der Versorgungseinrichtung wurde wiederhergestellt, nachdem die Bedingung **upsOnBattery** eingetreten war.	informational

Tabelle 20: APC-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
restartAgent	29	Der Agent wird auf ein Kommando des Verwaltungsprogramms hin erneut gestartet.	informational
returnFromBypass	23	Die USV hat den Überbrükkungsmodus wieder abgeschaltet.	informational
returnFromLowBattery	11	Die USV hat die Bedingung **lowBattery** zurückgegeben.	informational
smartAvrReducing	31	Die USV hat Smart-AVR-Spannungsreduzierung aktiviert.	minor
smartBoostOn	6	Die USV hat **SmartBoost** aktiviert.	minor
softwareBypass	21	Die USV wurde vom Benutzer über die Software oder über die UPS-Frontplatte auf Überbrükkung geschaltet.	minor
switchedBypass	22	Die USV wurde vom Benutzer über den Schalter an der Rückseite auf Überbrückung geschaltet.	minor
upsBatteryNeeds Replacement	17	Die Batterien der USV müssen sofort ausgetauscht werden.	major
upsDiagnosticsFailed	3	Interner Selbsttest der USV ist fehlgeschlagen.	major
upsDiagnosticsPassed	10	Interner Selbsttest der USV erfolgreich durchgeführt.	informational
upsDipSwitchChanged	16	DIP-Schaltereinstellungen der USV wurden geändert.	minor

Tabelle 20: APC-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
upsDischarged	4	Die Batterien der USV sind entladen. Wenn die Stromversorgung unterbrochen wird, tritt umgehend eine Bedingung niedrigen Ladezustands ein. Eine ausreichende Laufzeit für erforderliche Gegenmaßnahmen ist dann nicht gewährleistet.	major
upsOnBattery	5	Die USV liefert jetzt Strom für die Notstromversorgung.	minor
upsOverload	2	Die USV hat eine Auslastung ermittelt, die 100 Prozent ihrer eigenen Kapazität übersteigt.	major
upsRebootStarted	15	Die USV hat einen Warmstart eingeleitet. Die UPS startet sich zu diesem Zeitpunkt selbst erneut.	minor
upsSleeping	13	Die USV wechselt in den Modus **sleep**.	minor
upsTurnedOff	12	Die USV wurde von der Verwaltungsstation abgeschaltet.	minor
upsTurnedOn	30	Die USV ist aktiviert.	informational
upsWokeUp	14	Die USV hat den Modus **sleep** beendet. Die Stromversorgung wurde wieder hergestellt.	informational

Tabelle 20: APC-Traps

5.3.3 Blade System-Traps (s31.mib)

MIB-OID: 1.3.6.1.4.1.7244.1.1.1

Im Folgenden finden Sie eine alphabetische Übersicht über die Blade System-Traps.

Trap-Name	ID	Bedeutung	Fehlerklasse
s31LivetimeError	1644	Die Lebensdauer des Blade Systems wurde überschritten.	minor
s31MgmtBladeAdded	1601	Ein Management Blade wurde dem Blade System hinzugefügt.	informational
s31MgmtBladeCriticalError	1605	Der Status des Management Blades in dem Blade System ist kritisch.	critical
s31MgmtBladeError	1604	Der Status des Management Blades in dem Blade System ist fehlerhaft.	major
s31MgmtBladeOk	1603	Der Status des Management Blades in dem Blade System ist ok.	informational
s31MgmtBladeRemoved	1602	Ein Management Blade wurde aus dem Blade System entfernt.	informational
s31NicDetectionFail	1646	Bei einem Management Blade in dem Blade System ist bei der Net Work Interface Card (NIC)-Suche ein Fehler aufgetreten.	informational

Tabelle 21: Blade System-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
s31PowerOverBudget	1645	Der Server Blade eines Blade Systems konnte wegen Lastüberschreitung nicht eingeschaltet werden.	minor
s31ServerBladeAdded	1606	Ein Server Blade wurde dem Blade System hinzugefügt.	informational
s31ServerBladeCritical Error	1610	Der Status des Server Blades in dem Blade System ist kritisch.	critical
s31ServerBladeError	1609	Der Status des Server Blades in dem Blade System ist fehlerhaft.	major
s31ServerBladeHot Replace	1640	Ein Server Blade wurde im laufenden Betrieb ersetzt.	informational
s31ServerBladeNewAdd	1639	Dem Blade System wurde an einem freien Steckplatz ein Server Blade hinzugefügt.	informational
s31ServerBladeOk	1608	Der Status des Server Blades in dem Blade System ist ok.	informational
s31ServerBladeRemoved	1607	Ein Server Blade wurde aus dem Blade System entfernt.	informational
s31ServerBootError	1633	Auf dem Server Blade in dem Blade System wurde kein bootfähiges Betriebssystem gefunden.	informational
s31ServerBootWatchdog Expired	1636	Der BootWatchdog am Server Blade im Blade System ist beendet.	informational

Tabelle 21: Blade System-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
s31ServerPostError	1632	Der Status des Power On Self Tests des Server Blades im Blade System ist fehlerhaft.	informational
s31ServerPowerOff	1641	Der Server Blade ist ausgeschaltet.	informational
s31ServerPowerOn	1631	Der Server Blade im Blade System ist eingeschaltet.	informational
s31ServerShutdown	1634	Der Server Blade wurde heruntergefahren.	informational
s31ServerSoftware WatchdogExpired	1635	Der SoftwareWatchdog am Server Blade im Blade System ist beendet.	informational
s31SwitchBladeAdded	1611	Ein Switch Blade wurde dem Blade System hinzugefügt.	informational
s31SwitchBladeCritical Error	1615	Der Status des Switch Blades in dem Blade System ist kritisch.	critical
s31SwitchBladeError	1614	Der Status des Switch Blades in dem Blade System ist fehlerhaft.	major
s31SwitchBladeOk	1613	Der Status des Switch Blades in dem Blade System ist ok.	informational
s31SwitchBladeRemoved	1612	Ein Switch Blade wurde aus dem Blade System entfernt.	informational
s31SysFanAdded	1616	Ein Lüfter wurde dem Blade System hinzugefügt.	informational
s31SysFanCriticalError	1620	Der Status des Lüfters in dem Blade System ist kritisch.	critical

Tabelle 21: Blade System-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
s31SysFanError	1619	Der Status des Lüfters in dem Blade System ist fehlerhaft.	major
s31SysFanOk	1618	Der Status des Lüfters in dem Blade System ist ok.	informational
s31SysFanRemoved	1617	Ein Lüfter wurde aus dem Blade System entfernt.	informational
s31SysPowerSupplyAdded	1626	Ein Netzteil wurde dem Blade System hinzugefügt.	informational
s31SysPowerSupplyCriticalError	1630	Der Status des Netzteils in dem Blade System ist kritisch.	critical
s31SysPowerSupplyError	1629	Das Netzteil in dem Blade System ist ausgefallen.	major
s31SysPowerSupplyOk	1628	Das Netzteil in dem Blade System funktioniert wieder.	informational
s31SysPowerSupplyRemoved	1627	Ein Netzteil wurde aus dem Blade System entfernt.	informational
s31SysTempCriticalError	1623	Die Temperatur am System-Temperatursensor hat eine kritische Höhe erreicht.	critical
s31SysTempError	1622	Der Temperatur am System-Temperatursensor ist nicht in Ordnung.	major
s31SysTempOk	1621	Die Temperatur am System-Temperatursensor ist ok.	informational

Tabelle 21: Blade System-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
s31SysTempSensorAdded	1642	Ein Systemtemperatursensor wurde dem Blade System hinzugefügt.	informational
s31SysTempSensorBroken	1625	Der System-Temperatursensor des Blade Systems ist defekt oder nicht angeschlossen.	major
s31SysTempSensorOK	1624	Der System-Temperatursensor funktioniert wieder.	informational
s31SysTempSensor Removed	1643	Ein Systemtemperatursensor wurde aus dem Blade System entfernt.	informational
s31TestTrap	1600	Ein Test-Trap wurde vom Blade System gesendet (kein Fehler).	informational
s31TrapEventLog	1638	Am Blade System wurde ein Fehler aufgezeichnet. Weitere Information dazu entnehmen Sie dem Trap-Ereignisprotokoll (Recovery).	major
s31UserAuthentication Failure	1637	Am Blade System wurde eine fehlgeschlagene Benutzerauthentifizierung entdeckt. Durchführung des Protokolls.	major

Tabelle 21: Blade System-Traps

5.3.4 Cluster-Traps (NTCluster.mib)

MIB-OID: 1.3.6.1.4.1.231

Im Folgenden finden Sie eine alphabetische Übersicht über Cluster-Traps.

Trap-Name	ID	Bedeutung	Fehlerklasse
sniWpChange ClusterActiveAgain	811	Der SNMP-Agent hat die Verbindung mit dem Cluster-Service hergestellt.	informational
sniWpChange ClusterNoLonger Active	812	Der SNMP-Agent hat die Verbindung mit dem Cluster-Service verloren.	critical
sniWpChange ClusterNotFound Active	810	Der SNMP-Agent startete, konnte aber nicht mit dem Cluster-Service kommunizieren.	critical
sniWpChange GroupAdded	851	Eine neue Ressourcengruppe wurde erstellt.	informational
sniWpChange GroupDeleted	850	Eine Ressourcengruppe wurde gelöscht.	informational
sniWpChange GroupProperty	853	Die Einstellungen einer Ressourcengruppe wurden geändert.	informational
sniWpChange GroupState	852	Eine Ressourcengruppe hat ihren Status geändert.	informational
sniWpChange NetInterfaceAdded	921	Eine nEine neue Netzschnittstelle wurde erstellt.	informational
sniWpChange NetInterfaceDeleted	920	Eine Netzschnittstelle wurde gelöscht.	informational
sniWpChange NetInterfaceProperty	923	Die Einstellungen einer Netzschnittstelle haben sich geändert.	informational
sniWpChange NetInterfaceState	922	Eine Netzschnittstelle hat ihren Status geändert.	informational

Tabelle 22: Cluster-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
sniWpChange NetworkAdded	911	Ein Netz wurde dem Cluster hinzugefügt.	informational
sniWpChange NetworkDeleted	910	Ein Netz wurde aus dem Cluster entfernt.	informational
sniWpChange NetworkProperty	913	Die Einstellungen eines Netzes haben sich geändert.	informational
sniWpChange NetworkState	912	Ein Netz hat seinen Status geändert.	informational
sniWpChange NodeAdded	831	Ein neuer Knoten wurde dem Cluster hinzugefügt.	informational
sniWpChange NodeDeleted	830	Ein Knoten wurde dauerhaft aus dem Cluster entfernt.	informational
sniWpChange NodeState	832	Ein Cluster-Knoten hat seinen Status geändert.	informational
sniWpChange RegistryAttributes	895	Die Registrierungsschlüssel des Clusters wurden geändert.	informational
sniWpChange RegistryKey	896	Ein Registrierungsschlüssel des Clusters wurde erstellt oder gelöscht.	informational
sniWpChange RegistryValue	897	Ein Registrierungswert eines Clusters wurde geändert oder gelöscht.	informational
sniWpChange ResourceAdded	861	Eine neue Ressource wurde im Cluster erstellt.	informational
sniWpChange ResourceDeleted	860	Eine Cluster-Ressource wurde gelöscht.	informational
sniWpChange ResourceProperty	863	Die Einstellungen einer Cluster-Ressource wurden geändert.	informational
sniWpChange ResourceState	862	Eine Cluster-Ressource hat ihren Status geändert.	informational
sniWpChange ResourceTypeAdded	841	Eine neue Ressourcenart wurde erstellt.	informational

Tabelle 22: Cluster-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
sniWpChange ResourceType Deleted	840	Eine Ressourcenart wurde gelöscht.	informational
sniWpChange Unknown	801	Die Cluster-API hat eine Hinweisart zurückgegeben, für die derzeit kein anderer Trap definiert ist.	informational

Tabelle 22: Cluster-Traps

5.3.5 DPT-Traps (dptscsi.mib)

MIB-OID: 1.3.6.1.4.1.1597

Im Folgenden finden Sie eine alphabetische Übersicht über die DPT-Traps.

Trap-Name	ID	Bedeutung	Fehlerklasse
dptArrayCfgChangeTrap	12	Konfiguration eines RAIDArray auf Grund eines der folgenden Ereignisse: – Erstellen eines neuen Array. – Löschen eines vorhandenen Array. – Ändern eines Array (z.B. Ändern der Stripe-Größe, etc.).	informational
dptDevBlock ReassignedTrap	6	Die HBA hat einen Block erneut zugeordnet. **dptScsiDevBadBlockNumber** enthält die neu zugeordnete Blocknummer.	minor
dptDevData InconsistentTrap	7	Die RAID-Prüffunktion hat eine Dateninkonsistenz festgestellt. **dptScsiDevBadBlockNumber** und **dptScsiDevBadBlockCount** enthalten die Nummer des Startblocks sowie jeweils die Anzahl der betroffenen Blöcke.	informational
dptDevError ThresholdHitTrap	8	Der Status der jeweiligen Einheit hat sich geändert und die Fehlerzahl hat den Crash-Schwellwert für die Einheit erreicht.	informational

Tabelle 23: DPT traps

Trap-Name	ID	Bedeutung	Fehlerklasse
dptDevLocking StatusChangedTrap	10	Das Sperren des Laufwerks wurde gestartet/gestoppt.	informational
dptDevReqSenseTrap	11	Von der HBA wurde eine Anforderung nach Prüfinformationen empfangen.	informational
dptDevStatus ChangedTrap	9	Der Status der SCSI-Einheit hat sich geändert.	informational
dptHbaCorrected HardRAMErrorTrap	4	Die HBA hat einen ECCRAM-Fehler festgestellt und behoben. **dptScsiHbaBadMemoryAddress** enthält die RAM-Adresse.	informational
dptHbaSoftRAM ErrorTrap	3	Die HBA hat einen ECCRAM-Fehler festgestellt, der Fehler konnte jedoch nicht auf dem physischen Plattenblock gefunden werden. **dptScsiHbaBadMemoryAddress** enthält die RAM-Adresse.	informational
dptHbaTemperature ChangeTrap	2	Auf der HBA wurde die normale Temperatur wiederhergestellt.	informational
dptHbaUnCorrectable HardRAMErrorTrap	5	Die HBA hat einen ECCRAM-Fehler festgestellt, konnte den Fehler jedoch nicht beheben. **dptScsiHbaBadMemoryAddress** enthält die RAM-Adresse.	informational

Tabelle 23: DPT traps

Trap-Name	ID	Bedeutung	Fehlerklasse
dptHbaVoltage ChangeTrap	1	Auf der HBA wurde eine niedrige Spannung festgestellt.	major
dptUnknownErrorTrap	13	Entsprechend der Definition des Wertes für das Objekt **dptScsiEventInfo** ist ein Ereignis eingetreten.	informational

Tabelle 23: DPT traps

5.3.6 DuplexDataManager-Traps (Ddm.mib)

MIB-OID: 1.3.6.1.4.1.231.2.10.2

Im Folgenden finden Sie eine alphabetische Übersicht über die DDM-Traps.

Trap-Name	ID	Bedeutung	Fehlerklasse
FscDdmNewConfig	1400	Es wurde entweder eine neue DuplexWrite-Gruppe erzeugt oder nach Anforderung des Benutzers eine Platte einer bereits vorhandenen DuplexWrite-Gruppe hinzugefügt.	informational
FscDdmPieceRemoved	1401	Nach Anforderung des Benutzers wurde eine Platte aus einer DuplexWrite-Gruppe entfernt.	informational
FscDdmConfigRemoved	1402	Nach Anforderung des Benutzers wurde eine DuplexWrite-Gruppe entfernt.	informational
FscDdmStatusSet	1403	Nach Anforderung des Benutzers wurde der Status einer DuplexWrite-Platte gesetzt.	minor
FscDdmUpdateStatus	1404	Der Status einer DuplexWrite-Platte wurde aktualisiert.	minor
FscDdmPieceRecovered	1405	Der Wiederherstellungsprozess einer DuplexWrite-Gruppe wurde erfolgreich beendet.	informational

Tabelle 24: DDM-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
FscDdmRecoverAborted	1406	Nach Anforderung des Benutzers wurde der Wiederherstellungsprozess einer DuplexWrite-Gruppe abgebrochen.	minor
FscDdmReservationConflict	1407	Ein Reservierungskonflikt wurde festgestellt. Von jetzt an steht eine gesamte DuplexWrite-Gruppe nicht mehr zur Verfügung. Dies führt nur dann zu einem Fehler, wenn der Konflikt im Betrieb (nicht Initialisierung) der Gruppe aufgetreten ist.	major
FscDdmConfigChanged	1408	Bei einem wiederholten Lesen der Konfiguration durch den Treiber wurde eine veränderte Konfiguration festgestellt.	informational
FscDdmConfigInvalidated	1409	Die Konfigurationsinformationen einer DuplexWrite-Gruppe wurden für ungültig erklärt. Die Konfigurationsinformationen werden vor dem nächsten Zugriff auf die DuplexWrite-Gruppe auf diesem Clusterelement erneut gelesen.	informational
FscDdmActiveLunChanged	1410	Eine bestimmte Platte wurde für Lesebefehle aus einer DuplexWrite-Gruppe ausgewählt.	informational
FscDdmPieceFailed	1411	Ein Fehler wurde auf einer DuplexWrite-Gruppe festgestellt.	critical

Tabelle 24: DDM-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
FscDdmRootFlagChanged	1412	Das RootDisk-Verhalten einer DuplexWrite-Gruppe wurde geändert.	informational
FscDdmForceActive	1413	Eine Platte einer DuplexWrite-Gruppe wurde durch den Treiber beim Reboot als zwingend aktiv markiert. Die Partner-Platte kann als Snapshot verwendet werden.	informational
FscDdmNameChanged	1414	Der Name einer DuplexWrite-Gruppe wurde geändert.	informational
FscDdmPathFailed	1415	Ein Fehler wurde auf einem Pfad einer MultiPath-Gruppe entdeckt.	critical
FscDdmRetry	1416	Ein Fehler wurde auf einem Pfad einer MultiPath-Gruppe entdeckt, und die Wiederholung der Anweisung war auf einem anderen Pfad erfolgreich.	major
FscDdmActivePortChanged	1417	Der aktive Pfad einer MultiPath-Gruppe wurde geändert.	informational
FscDdmReconfigured	1418	Eine Änderung wurde in der MultiPath-Konfiguration festgestellt.	informational
FscDdmStatusChanged	1419	Der Status eines MultiPath-Pfads wurde geändert.	informational
FscDdmAutoRecovered	1420	Ein Pfad einer MultiPath-Gruppe wurde aktiviert (AutoRecovery).	informational

Tabelle 24: DDM-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
FscDdmErrorCleared	1421	Der Fehlerstatus eines MultiPath-Pfads wurde gelöscht.	informational
FscDdmPnPRemove	1422	Ein Plug-and-Play-Gerät wurde entfernt.	informational
FscDdmPnPNew	1423	Ein Plug-and-Play-Gerät wurde hinzugefügt.	informational
FscDdmDdmCluster	1424	Eine Änderung der Clusterkonfiguration wurde durch den DuplexDataManager-Dienst festgestellt.	informational

Tabelle 24: DDM-Traps

5.3.7 DuplexWrite-Traps (DW.mib)

MIB-OID: 1.3.6.1.4.1.231.2.10.2

Im Folgenden finden Sie eine alphabetische Übersicht über die DuplexWrite Traps.

Trap-Name	ID	Bedeutung	Fehlerklasse
sieDWActiveLunChanged	1310	Der Benutzer hat den Lesepfad für eine DuplexWrite-Gruppe ausdrücklich auf eine bestimmte Platte festgelegt.	informational
sieDWConfig Changed	1308	Bei einem wiederholten Lesen der Konfiguration durch den Treiber wurde eine veränderte Konfiguration festgestellt.	informational
sieDWConfigInvalidated	1309	Der DuplexWrite-Cluster-Dienst hat die Konfigurationsinformation einer Platte für ungültig erklärt. Vor dem nächsten Zugriff auf diese Platte auf diesem Cluster-Element wird die Konfigurationsinformation neu gelesen.	informational
sieDWDiskRegistered	1351	Ein Benutzer hat die Verwendung einer Platte für DuplexWrite durch Veränderung der Registrierung gesperrt oder freigegeben. Diese Einstellung wird für den Treiber erst nach einem Neustart des Systems wirksam.	informational

Tabelle 25: DuplexWrite-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
sieDWConfigRemoved	1302	Ein Benutzer hat eine DuplexWrite-Gruppe entfernt. Diese Aktion wurde auf Anforderung des Konfigurationsdienstprogramms durchgeführt.	informational
sieDWNewConfig	1300	Ein Benutzer hat eine neue DuplexWrite-Gruppe erstellt oder eine Platte zu einer existierenden DuplexWrite-Gruppe hinzugefügt. Diese Aktion wurde auf Anforderung des Konfigurationsdienstprogramms durchgeführt.	informational
sieDWPieceFailed	1311	Der Treiber hat einen Fehler auf einer Platte einer DuplexWrite-Gruppe festgestellt.	critical
sieDWPieceRecovered	1305	Die Wiederherstellung einer DuplexWrite-Gruppe wurde erfolgreich abgeschlossen. Beide Elemente der DuplexWrite-Gruppe befinden sich im Status ONLINE.	informational
sieDWPieceRemoved	1301	Ein Benutzer hat eine Platte aus einer DuplexWrite-Gruppe entfernt. Diese Aktion wurde auf Anforderung des Konfigurationsdienstprogramms durchgeführt.	informational
sieDWRecoverAborted	1306	Die Wiederherstellung einer DuplexWrite-Gruppe wurde von einem Benutzer abgebrochen.	minor

Tabelle 25: DuplexWrite-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
sieDWRefreshFinished	1350	Die internen Datenstrukturen wurden von der Treiberschnittstelle aktualisiert.	informational
sieDWReservationConflict	1307	Der Treiber hat einen Reservierungskonflikt festgestellt. Eine ganze DuplexWrite-Gruppe ist nicht mehr zugreifbar. Dies ist kein Fehler während der Initialisierungsphase.	major
sieDWStatusSet	1303	Ein Benutzer hat den Status einer Platte einer DuplexWrite-Gruppe geändert. Diese Aktion wurde auf Anforderung des Konfigurationsdienstprogramms durchgeführt.	minor
sieDWUpdateStatus	1304	Der Status einer DuplexWrite-Gruppe wurde vom Treiber aktualisiert.	minor

Tabelle 25: DuplexWrite-Traps

5.3.8 Festplatten-Traps (S.M.A.R.T.) (Hd.mib)

Im Folgenden finden Sie eine alphabetische Übersicht über die Festplatten-Traps.

MIB-OID: 1.3.6.1.4.1.231.2.10.2

Trap-Name	ID	Bedeutung	Fehlerklasse
sniSMARTFailure Predicted	750	S.M.A.R.T. gibt eine Warnung aus, dass möglicherweise ein Festplattenlaufwerk ausfällt.	critical
sniSMARTMonitoring Disabled	751	Die S.M.A.R.T.-Konfiguration wurde geändert.	informational

Tabelle 26: Festplatten-Traps

5.3.9 Generische Traps

Im Folgenden finden Sie eine alphabetische Übersicht über generische Traps.

Trap-Name	ID	Bedeutung	Fehlerklasse
coldStart	0	Ein Agent wurde erneut gestartet. MIB-Anzeigenobjekte haben sich möglicherweise geändert.	minor
egpNeighborLoss	5	Ein EGP-Nachbarknoten des verwalteten Knotens hat vom Status **UP** in den Status **DOWN** gewechselt.	major
linkDown	2	Eine Schnittstelle des verwalteten Knotens hat vom Status **UP** in den Status **DOWN** gewechselt.	critical
linkUp	3	Eine Schnittstelle des verwalteten Knotens hat vom Status **DOWN** in den Status **UP** gewechselt.	minor
warmStart	1	Agent erneut initialisiert, Objekte unverändert.	minor

Tabelle 27: Generische Traps

5.3.10 MultiPath-Traps (mp.mib)

MIB-OID: 1.3.6.1.4.1.231.2.10.2

Im Folgenden finden Sie eine alphabetische Übersicht über MultiPath-Traps.

Trap-Name	ID	Bedeutung	Fehlerklasse
sieMP ActivePortChanged	1202	Der Benutzer hat einen Pfad einer MultiPath-Gruppe an- oder ausgeschaltet.	informational
sieMPAutoRecovered	1205	Durch automatisches Wiederherstellen ist ein vorher im Fehlerstatus befindlicher Pfad einer MultiPath-Gruppe wieder zugreifbar.	informational
sieMPError	1200	Eine MultiPath-Gruppe besteht nur noch aus einem Pfad und auf diesem wurde ein Fehler festgestellt. Die MultiPath-Gruppe ist nicht mehr arbeitsfähig.	critical
sieMPErrorCleared	1206	Ein Benutzer hat den Fehlerstatus eines Pfades einer MultiPath-Gruppe gelöscht.	informational
sieMPReconfigured	1203	Bei einer MultiPath-Gruppe wurde ein Pfad entfernt oder hinzugefügt.	informational
sieMPRetry	1201	In einem Pfad einer MultiPath-Gruppe wurde ein Fehler festgestellt. Es wird versucht, das Kommando auf einem anderen Pfad der MultiPath-Gruppe auszuführen.	critical

Tabelle 28: MultiPath-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
sieMPStatusChanged	1204	Ein Benutzer hat eine Änderung an einer MultiPath-Gruppe vorgenommen (automatisches Wiederherstellen ein/aus, Lastausgleich ein/aus, Pfad aktivieren/inaktivieren).	informational

Tabelle 28: MultiPath-Traps

5.3.11 Mylex-Traps (Mylex.mib)

MIB-OID: 1.3.6.1.4.1.231.2.10.2

Im Folgenden finden Sie eine alphabetische Übersicht über die Mylex-Traps.

Trap-Name	ID	Bedeutung	Fehlerklasse
mylexAdapterDied	221	Verbindung zur Steuereinheit einer Platteneinheit unterbrochen.	critical
mylexAutoRebuild Started	200	Automatische Wiederherstellung einer Einheit wurde gestartet.	critical
mylexAutoRebuild Started2	222	Automatische Wiederherstellung eines Systemlaufwerks wurde gestartet.	informational
mylexBBUFound	275	Batteriesicherungseinheit festgestellt.	informational
mylexBBUPowerLow	276	Ladezustand der Batteriesicherungseinheit ist niedrig.	critical
mylexBBUPowerOK	277	Ladezustand der Batteriesicherungseinheit ist in Ordnung.	informational

Tabelle 29: Mylex-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
mylexGamDriver IncorrectVersion	262	Fehlerhafte Version eines GAM-Treibers installiert.	minor
mylexGamDriverMissing	261	GAM-Treiber ist entweder nicht installiert oder nicht gestartet.	minor
mylexInitialization Cancelled	231	Initialisierung des Systemlaufwerks abgebrochen.	informational
mylexInitializationDone	230	Initialisierung des Systemlaufwerks erfolgreich abgeschlossen.	informational
mylexInitializationFailed	232	Initialisierung des Systemlaufwerks fehlgeschlagen.	major
mylexInitializationStarted	229	Initialisierung des Systemlaufwerks gestartet.	informational
mylexLogicalDriveCritical	215	Ein logisches Laufwerk befindet sich in einem kritischen Zustand. Ein Laufwerk einer RAIDKonfiguration ist ausgefallen.	major
mylexLogicalDriveOffline	214	Ein logisches Laufwerk ist offline.	critical
mylexLogicalDriveOnline	216	Ein logisches Laufwerk ist online.	critical
mylexManualRebuild Started	201	Manuelle Wiederherstellung ist gestartet.	informational

Tabelle 29: Mylex-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
mylexManualRebuild Started2	223	Manuelle Wiederherstellung ist gestartet. Nach erfolgreicher Wiederherstellung wird **mylexRebuildDone2** gesendet.	informational
mylexParityCheck Cancelled	210	Paritätsprüfung wurde abgebrochen.	informational
mylexParityCheckDone	209	Paritätsprüfung ist erfolgreich abgeschlossen.	informational
mylexParityCheckError	212	Ein Paritätsprüfungsfehler wurde ermittelt.	major
mylexParityCheck LogicalDriveFailed	213	Paritätsprüfung: logisches Laufwerk ausgefallen	major
mylexParityCheckStarted	208	Paritätsprüfung gestartet.	informational
mylexParityCheckStatus	211	Paritätsprüfungsstatus	informational
mylexPhysicalDevice Added	257	Physische Einheit hinzugefügt.	informational
mylexPhysicalDevice Alive	218	Physische Einheit ist online.	informational
mylexPhysicalDevice Died	217	Physische Einheit ist abgeschaltet.	critical
mylexPhysicalDevice HardError	251	Permanenter Fehler in physischer Einheit.	minor
mylexPhysicalDevice Hotspare	250	Bei der physischen Einheit handelt es sich jetzt um eine Hotspare-Einheit.	informational
mylexPhysicalDevice MiscError	254	Allgemeiner Fehler in physischer Einheit.	minor
mylexPhysicalDevice ParityError	253	Paritätsfehler in physischer Einheit.	minor
mylexPhysicalDevice Prefailure	255	Warnung von physischer Einheit vor einem Fehler.	major

Tabelle 29: Mylex-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
mylexPhysicalDevice Removed	258	Physische Einheit wurde entfernt.	major
mylexPhysicalDevice SoftError	252	Normaler Fehler in physischer Einheit.	minor
mylexPhysicalDevice Unconfigured	256	Physische Einheit ist nicht konfiguriert.	minor
mylexRaidExpansion Done	236	Erweiterung der RAIDKapazität erfolgreich abgeschlossen.	minor
mylexRaidExpansion Failed	237	Erweiterung der RAIDKapazität fehlgeschlagen.	major
mylexRaidExpansion Started	235	Erweiterung der RAIDKapazität gestartet.	informational
mylexRaidTypeChanged	240	RAID-Art des Systemlaufwerks wurde geändert.	informational
mylexRebuildCancelled	203	Wiederherstellung abgebrochen.	informational
mylexRebuildCancelled2	225	Wiederherstellung des Systemlaufwerks abgebrochen.	informational
mylexRebuildDone	202	Wiederherstellung erfolgreich abgeschlossen.	informational
mylexRebuildDone2	224	Wiederherstellung des Systemlaufwerks erfolgreich abgeschlossen.	informational
mylexRebuildError	205	Wiederherstellungsfehler ermittelt.	major
mylexRebuildError2	226	Wiederherstellungsfehler im Systemlaufwerk ermittelt.	major

Tabelle 29: Mylex-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
mylexRebuildLogical DriveFailed	207	Wiederherstellung am Adapter der Platteneinheit abgeschlossen; fehlerhafte Blöcke ermittelt.	major
mylexRebuildLogical DriveFailed2	228	Wiederherstellung des Systemlaufwerks abgeschlossen; Systemlaufwerk auf dem Server ausgefallen.	major
mylexRebuildNew DeviceFailed	206	Wiederherstellung abgeschlossen; neue Einheit ausgefallen.	major
mylexRebuildNewDevice Failed2	227	Wiederherstellung des Systemlaufwerks; neue Einheit ausgefallen.	major
mylexRebuildStatus	204	Wiederherstellungsstatus	informational
mylexSMART ConfigurationChanged	271	S.M.A.R.T.-Konfiguration wurde geändert.	informational
mylexSMART FailurePredicted	270	Wird gesendet, wenn auf einem physischen Laufwerk ein Fehler (S.M.A.R.T.) vorhergesagt wurde.	critical
mylexStateChange TableFull	220	Cache-Änderungstabelle ist voll. Seit dem letzten Warmstart wurden zu viele Konfigurationsänderungen vorgenommen.	major
mylexSystemDriveBad Block	238	Fehlerhafter Block auf Systemlaufwerk ermittelt.	minor
mylexSystemDrive Created	233	Systemlaufwerk erstellt.	informational
mylexSystemDrive Deleted	234	Systemlaufwerk gelöscht.	informational
mylexSystemDrive SizeChanged	239	Größe des Systemlaufwerks geändert.	informational

Tabelle 29: Mylex-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
mylexWriteBackError	219	Rückschreibfehler im Cache der Steuereinheit.	major
mylexWriteBackError2	260	Rückschreibfehler im Cache der Steuereinheit.	major

Tabelle 29: Mylex-Traps

5.3.12 PCI-HotPlug-Traps (pcihotplug.mib)

MIB-OID: 1.3.6.1.4.1.231.2.10.2

Im Folgenden finden Sie eine alphabetische Übersicht über die PCI-HotPlug-Traps.

Trap-Name	ID	Bedeutung	Fehlerklasse
sieDeviceHotPlug TrapHotAdd	1022	Eine SCSI-Einheit wurde hinzugefügt.	informational
sieDeviceHotPlug TrapHotRemoval	1020	Eine SCSI-Einheit wurde entfernt.	informational
sieDeviceHotPlug TrapHotReplace	1021	Eine SCSI-Einheit wurde ausgetauscht.	informational
siePciHotPlugTrap EndHotPlugAction	1002	Die HotPlug-Aktion für die physikalische Steckplatznummer im Objekt **pciHotPlugTrapPhysicalSlotNumber** wurde fertiggestellt.	informational
siePciHotPlugTrap HotRemoval	1000	Ein Entfernen einer Einheit im laufenden Betrieb (Hot Removal) wurde gestartet.	informational
siePciHotPlugTrap HotReplace	1001	Ein Austauschen einer Einheit im laufenden Betrieb (Hot Replace) wurde gestartet.	informational

Tabelle 30: PCI-HotPlug-Traps

5.3.13 PRIMEPOWER-Traps

Im Folgenden finden Sie eine Beschreibung der von PRIMEPOWER gelieferten Traps.

ADICLIBMIB-V2 traps (ADICLIBMIB-v2.mib)

MIB-OID: 1.3.6.1.4.1.3764.3

Trap-Name	ID	Bedeutung	Fehlerklasse
doorStateChange	2	Der Status einer Tür hat sich verändert.	informational
error	6	Ein Gerät hat einen Fehler. Fehlercode und -daten werden ausgegeben.	informational
mailboxStateChange	3	Der Status einer Mailbox hat sich verändert.	informational
sac	7	Ein Gerät hat einen SAC-Code erzeugt.	informational
shutdown	5	Ein Gerät wurde heruntergefahren. Der Status des Shutdown wird ausgegeben.	informational
startup	4	Ein Gerät wurde gestartet. Der Status des Shutdown wird ausgegeben.	informational
statusChange	1	Ein Status hat sich geändert. Der vorherige Status wird ausgeben.	informational

Tabelle 31: Traps der ADICLIBMIB

Traps der DOMAIN-MIB (domagt.mib)

MIB-OID: 1.3.6.1.4.1.231.2.41

Trap-Name	ID	Bedeutung	Fehlerklasse
domNodeAdded	52	Ein Client wurde der Domäne hinzugefügt.	informational
domNodeDeleted	53	Ein Client wurde entfernt.	informational
domNodeOffline	50	Ein Client ging offline.	informational
domNodeOnline	51	Ein Client ging online.	informational
domNoManagementServer	55	Ein Agent wurde angehalten.	informational
domStartTrap	54	Ein Agent wurde gestartet.	informational

Tabelle 32: DOMAIN-MIB traps

Traps der FSC-LOG3-MIB (log3v1.mib)

MIB-OID: 1.3.6.1.4.1.231.2.46.2

Trap-Name	ID	Bedeutung	Fehlerklasse
log3AlertNotice	2	Ein LOG3-Event ist aufgetreten. Das System, der Modul, der Fehler und ein Text werden ausgegeben.	critical
log3CriticalNotice	3	Ein LOG3-Event ist aufgetreten. Das System, der Modul, der Fehler und ein Text werden ausgegeben.	critical
log3DebugNotice	8	Ein LOG3-Event ist aufgetreten. Das System, der Modul, der Fehler und ein Text werden ausgegeben.	informational
log3EmergencyNotice	1	Ein LOG3-Event ist aufgetreten. Das System, der Modul, der Fehler und ein Text werden ausgegeben.	critical

Tabelle 33: FSC-LOG3-MIB traps

Trap-Name	ID	Bedeutung	Fehlerklasse
log3ErrorNotice	4	Ein LOG3-Event ist aufgetreten. Das System, der Modul, der Fehler und ein Text werden ausgegeben.	major
log3InformationalNotice	7	Ein LOG3-Event ist aufgetreten. Das System, der Modul, der Fehler und ein Text werden ausgegeben.	informational
log3NoticeNotice	6	Ein LOG3-Event ist aufgetreten. Das System, der Modul, der Fehler und ein Text werden ausgegeben.	informational
log3OtherNotice	9	Ein LOG3-Event ist aufgetreten. Das System, der Modul, der Fehler und ein Text werden ausgegeben.	informational
log3WarningNotice	5	Ein LOG3-Event ist aufgetreten. Das System, der Modul, der Fehler und ein Text werden ausgegeben.	minor

Tabelle 33: FSC-LOG3-MIB traps

Traps der UNISERV-MIB (uniserv.mib)

MIB-OID: 1.3.6.1.4.1.231.2.41

Trap-Name	ID	Bedeutung	Fehlerklasse
kaiPartitionOffline	700	Eine Partition wurde abgeschaltet.	minor
kaiPartitionOnline	701	Eine Partition wurde eingeschaltet.	informational

Tabelle 34: UNISERV-MIB traps

Traps der PRIMEPOWER-XSCF-MIB (primepower_xscf.mib)

MIB-OID: 1.3.6.1.4.1.211.1.15.2.1

Trap-Name	ID	Bedeutung	Fehlerklasse
scfAgentStart	5	Der XSCF-Agent wurde gestartet.	informational
scfHardwareDefectRepair	7	Ein Hardwaredefekt wurde behoben.	minor
scfHardwareDefectSet	1	Ein Hardwaredefekt ist aufgetreten.	critical
scfHardwareDefectUnset	2	Ein Hardwaredefekt wurde zurückgesetzt.	informational
scfHardwareErrorRepair	6	Ein Hardwarefehler wurde behoben.	minor
scfHardwareErrorSet	3	Ein Hardwarefehler ist aufgetreten.	critical
scfHardwareErrorUnset	4	Ein Hardwarefehler wurde behoben.	informational

Tabelle 35: PRIMEPOWER-XSCF-MIB traps

Traps der FSC-HACL-MIB (v1_fscHaCl.mib)

MIB-OID: 1.3.6.1.4.1.231.2.42.2.0

Trap-Name	ID	Bedeutung	Fehlerklasse
fscHaClApplicationStateChanged	5	Der Status einer Applikation hat sich verändert.	major
fscHaClClusterInfAvailable	1	Informationen zu einem Cluster sind verfügbar. InfoOperScope wird ausgegeben.	informational
fscHaClClusterInfNotAvailable	2	Informationen zu einem Cluster sind nicht mehr verfügbar. InfoOperScope wird ausgegeben.	major
fscHaClMonitorStateChanged	3	Der Überwachungsstatus eines Clusters hat sich geändert.	major

Tabelle 36: FSC-HACL-MIB traps

Trap-Name	ID	Bedeutung	Fehlerklasse
fscHaClResourceStateChanged	6	Der Status einer Ressource hat sich verändert.	minor
fscHaClSystemStateChanged	4	Der Systemstatus hat sich verändert.	critical

Tabelle 36: FSC-HACL-MIB traps

Traps der WSA-TRAP-MIB (wsatrap.mib)

MIB-OID: 1.3.6.1.4.1.231.2.41

Trap-Name	ID	Bedeutung	Fehlerklasse
testTrap	600	Ein Testtrap wurde vom Server gesendet (kein Fehler).	informational
wsaAgentStart	5	Der WSA-Agent wurde gestartet.	informational
wsaControllerHardwareDefectSet	307	An einem Controller ist ein Hardwaredefekt aufgetreten.	critical
wsaControllerHardwareErrorSet	308	An einem Controller ist ein Hardwarefehler aufgetreten.	critical
wsaControllerRepair	309	Ein Controller wurde repariert.	minor
wsaDefectRepair	7	Ein Defekt wurde behoben.	minor
wsaDROperationStarted	312	Eine DR-Operation wurde gestartet.	informational
wsaDROperationFinished	313	Eine DR-Operation wurde beendet.	informational
wsaEnvironmentHardwareDefectSet	301	An einem Peripheriegerät ist ein Hardwaredefekt aufgetreten.	critical

Tabelle 37: WSA-TRAP-MIB traps

Trap-Name	ID	Bedeutung	Fehlerklasse
wsaEnvironmentHardwareErrorSet	302	An einem Peripheriegerät ist ein Hardwarefehler aufgetreten.	critical
wsaEnvironmentRepair	303	Ein Peripheriegerät wurde repariert.	minor
wsaErrorRepair	6	Ein Fehler wurde behoben.	minor
wsaGenLogMessage	900	An einem Server ist in einem Modul ein Fehler aufgetreten.	informational
wsaGenLogMessageInfo	910	An einem Server ist in einem Modul ein Fehler aufgetreten.	informational
wsaGenLogMessageCritical	913	An einem Server ist in einem Modul ein Fehler aufgetreten.	critical
wsaGenLogMessageMajor	912	An einem Server ist in einem Modul ein Fehler aufgetreten.	major
wsaGenLogMessageMinor	911	An einem Server ist in einem Modul ein Fehler aufgetreten.	minor
wsaHardwareActiveSet	315	Hardware Active wurde gesetzt.	informational
wsaHardwareDeactiveSet	314	Hardware Deactive wurde gesetzt.	critical
wsaHWComponentAttached	316	Eine Hardwarekomponente wurde angeschlossen.	informational
wsaHWComponentDetached	317	Eine Hardwarekomponente wurde entfernt.	informational
wsaLarHardwareDefectSet	1	Ein Hardwaredefekt ist aufgetreten.	critical
wsaLarHardwareDefectUnset	2	Ein Hardwaredefekt wurde behoben.	informational

Tabelle 37: WSA-TRAP-MIB traps

Trap-Name	ID	Bedeutung	Fehlerklasse
wsaLarHardwareErrorSet	3	Ein Hardwarefehler ist aufgetreten.	critical
wsaLarHardwareErrorUnset	4	Ein Hardwarefehler wurde behoben.	informational
wsaLUNStateChanged	101	Der Status einer Logical Unit Number hat sich geändert.	critical
wsaMonitoringRuleInitialized	311	Das EEM-Regelwerk wurde aktiviert.	minor
wsaMonitoringRuleMatched	310	Das EEM-Regelwerk wurde angepasst.	informational
wsaNodeStatusIntegrated	24	Ein Netzknoten wurde integriert.	informational
wsaNodeStatusNotavail	25	Ein Netzknoten ist nicht verfügbar.	critical
wsaNodeStatusNotrunning	26	Ein Netzknoten läuft nicht.	critical
wsaRAIDControllerDefect	102	Ein RAID-Controller ist defekt.	critical
wsaRAIDDiskDefect	103	An einem Server ist eine RAID-Disk defekt.	critical
wsaStorageHardwareDefectSet	304	An einer Storagekomponente ist ein Hardwaredefekt aufgetreten.	critical
wsaStorageHardwareErrorSet	305	An einer Storagekomponente ist ein Hardwarefehler aufgetreten.	critical
wsaStorageRepair	306	Eine Storagekomponente wurde repariert.	minor

Tabelle 37: WSA-TRAP-MIB traps

5.3.14 PXRE-Traps (dec.mib)

MIB-OID: 1.3.6.1.4.1.36.2.15.21

Im Folgenden finden Sie eine alphabetische Übersicht über die PXRE-Traps.

Trap-Name	ID	Bedeutung	Fehlerklasse
cacheBatteryFailureTrap	7	Die Cache-Batterie einer Steuereinheit ist ausgefallen. Cache-Batterie ersetzen oder wiederaufladen.	major
cacheBattery InformationTrap	9	Die Cache-Batterie einer Steuereinheit weist den Status **GOOD** auf.	informational
cacheBatteryLowTrap	8	Die Cache-Batterie einer Steuereinheit weist den Status **LOW** auf. Cache-Batterie ersetzen oder wiederaufladen.	minor
communication FailureTrap	12	Die Kommunikation mit dem Subsystem ist ausgefallen. Mögliche Ursachen: Unterbrechung des Datenpfades, Fehler bei der Kommunikation mit der LUN, Ausfall von 2 oder mehr Netzteilen, Ausfall von 2 oder mehr Lüftern, Überschreitung der maximalen Temperatur, beide Steuer-einheiten ausgefallen.	critical
communicationInformatio nTrap	13	Die Kommunikation mit dem Subsystem wurde wiederhergestellt.	informational

Tabelle 38: PXRE-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
controllerFailureTrap	14	Die sekundäre Steuereinheit im Subsystem ist ausgefallen. Die Steuereinheit muss ausgetauscht werden. Mögliche Ursachen: Ausgabe der PCMCIA-Speicherkarte, physisches Entfernen der Steuereinheit, Hardwarefehler.	major
controllerInformationTrap	15	Die sekundäre Steuereinheit im Subsystem wurde wiederhergestellt.	informational

Tabelle 38: PXRE-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
diskFailureTrap	1	Die sekundäre Steuereinheit im Subsystem wurde wiederhergestellt. Die Position dieses Laufwerks ist durch den Plattennamen angegeben. Die Platteneinheit muss ausgetauscht werden. Die im Namen enthaltenen Zahlen geben den Anschluss, die Zieladresse und die LUN des Steuereinheitenpaares an. Beispiele: – DISK10100 gibt die Position des Plattenlaufwerks an Anschluss 1, Zieladresse 01 und LUN 00 an. – DISK30300 gibt die Position des Plattenlaufwerks an Anschluss 3, Zieladresse 03 und LUN 00 an.	major

Tabelle 38: PXRE-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
diskInformationTrap	2	Ein Plattenlaufwerk wurde wiederhergestellt. Die Position dieses Laufwerks ist durch den Plattennamen angegeben. Die im Namen enthaltenen Zahlen geben den Anschluss, die Zieladresse und die LUN des Steuereinheitenpaares an. Beispiele: – DISK10100 gibt die Position des Plattenlaufwerks an Anschluss 1, Zieladresse 01 und LUN 00 an. – DISK30300 gibt die Position des Plattenlaufwerks an Anschluss 3, Zieladresse 03 und LUN 00 an.	informational
externalInputFailureTrap	20	Die benutzerdefinierte externe Eingabeeinheit zur EMU zeigt einen Fehler an. Wenn der Status **FAILURE** lautet, wurde an einer der benutzerdefinierten externen Eingabeeinheiten ein Fehler protokolliert.	major
externalInput InformationTrap	21	Die benutzerdefinierte externe Eingabeeinheit zur EMU zeigt einen Wiederherstellungsvorgang an.	informational

Tabelle 38: PXRE-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
fanFailureTrap	5	Der Lüfter an der angegebenen Position ist ausgefallen. Er muss ausgetauscht werden.	major
fanInformationTrap	6	Der Lüfter an der angegebenen Position wurde wiederhergestellt.	informational
lunFailureTrap	16	Die LUN ist ausgefallen und arbeitet offline. Mögliche Ursachen: zu viele ausgefallene Plattenlaufwerke, aus denen sich die LUN zusammensetzt oder das Betriebssystem kann aus anderen Gründen nicht mehr mit der LUN kommunizieren.	critical
lunInformationTrap	19	Eine LUN arbeitet wieder optimal, da der Wiederherstellungsvorgang erfolgreich abgeschlossen werden konnte.	informational

Tabelle 38: PXRE-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
lunReconstructTrap	17	Die LUN hat den Wiederherstellungsvorgang gestartet, kann jedoch weiterhin verwendet werden. Mögliche Ursachen: ein verfügbares Plattenlaufwerk wurde als Ersatzlaufwerk erstellt, das in der Gruppe hinzugefügt werden soll, ein vorhandenes Ersatzlaufwerk wurde automatisch in der Gruppe hinzugefügt, um bei einem Fehler an einer vorhandenen Platteneinheit den Wiederherstellungsvorgang einleiten zu können.	minor
lunReducedTrap	18	Eine LUN weist auf Grund eines Fehlers an einer Platteneinheit Leistungsmängel auf. Die fehlerhafte Platteneinheit muss ausgetauscht werden. Aus Gründen der Wiederherstellung muss ein Ersatzlaufwerk im System hinzugefügt werden.	major
powerSupplyFailureTrap	3	Das Netzteil an der angegebenen Position ist ausgefallen. Das Netzteil muss ausgetauscht werden.	major
powerSupply InformationTrap	4	Das Netzteil wurde wiederhergestellt.	informational

Tabelle 38: PXRE-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
temperature InformationTrap	11	Ein Temperaturfühler zeigt eine Temperatur unter dem Schwellwert **WARNING** an.	informational
temperatureOver ThresholdTrap	10	Ein Temperaturfühler zeigt eine höhere Temperatur als der Schwellwert **WARNING** an. Die Umgebungstemperatur muss verringert oder der interne Schwellwert muss angehoben werden (je nach Anwendung).	major

Tabelle 38: PXRE-Traps

5.3.15 RAID-Adapter-Traps (Megaraid.mib)

MIB-OID: 1.3.6.1.4.1.16.1.1.200

Im Folgenden finden Sie eine alphabetische Übersicht über die RAID-Adapter-Traps.

Trap-Name	ID	Bedeutung	Fehlerklasse
rtBatteryMissing	9020	Adapter-**%d**: Batteriemodul fehlt.	informational
rtBattery TemperatureHigh	9022	Adapter-**%d**: Temperatur des Batteriemoduls hat den Schwellwert Danger überschritten.	informational
rtBatteryVolatageLow	9021	Adapter-**%d**: Spannung des Batteriemoduls ist niedrig.	informational
rtCheck ConditionStatus	9018	Adapter-**%d**, Kanal-**%d**, Ziel-**%d**: Das Kommando wurde abgeschlossen mit Prüfschlüssel-**0x%x** ASC-**0x%x** ASCQ-**0x%x**.	informational
rtCheck ConsistencyAborted	9010	Adapter-**%d**, Logisches Laufwerk-**%d**: Konsistenzprüfung vom Benutzer abgebrochen.	informational
rtCheck ConsistencyCompleted	9009	Adapter-**%d**, Logisches Laufwerk-**%d**: Konsistenzprüfung abgeschlossen. Keine Inkonsistenzen festgestellt.	informational
rtCheck ConsistencyFailed	9012	Adapter-**%d**, Logisches Laufwerk-**%d**: Konsistenzprüfung gescheitert.	informational
rtCheck ConsistencyStarted	9008	Adapter-**%d**, Logisches Laufwerk-**%d**: Konsistenzprüfung gestartet.	informational

Tabelle 39: RAID-Adapter-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
rtConfigUpdated	9001	Adapter-**%d**: Es wurde eine neue Konfiguration geschrieben.	informational
rtConsistency Corrected	9011	Adapter-**%d**, Logisches Laufwerk-**%d**: Konsistenzprüfung abgeschlossen. Inkonsistenzen wurden behoben.	informational
rtInitializeAborted	9006	Adapter-**%d**, Logisches Laufwerk-**%d**: Initialisierung vom Benutzer abgebrochen.	informational
rtInitializeCompleted	9005	Adapter-**%d**, Logisches Laufwerk-**%d**: Initialisierung erfolgreich abgeschlossen.	informational
rtInitializeFailed	9007	Adapter-**%d**, Logisches Laufwerk-**%d**: Initialisierung gescheitert.	informational
rtInitializeStarted	9004	Adapter-**%d**, Logisches Laufwerk-**%d**: Initialisierung gestartet.	informational
rtLogicalDrive StateChange	9003	Adapter-**%d**, Logisches Laufwerk-**%d**: Status hat sich von **%s** in **%s** geändert.	informational
rtNewDriveInserted	9019	Adapter-**%d**, Kanal-**%d**, Ziel-**%d**: Neue Einheit eingefügt.	informational
rtPhysicalDrive StateChange	9002	Adapter-**%d**, Kanal-**%d**, Ziel-**%d**: Laufwerkstatus hat sich von **%s** in **%s** geändert.	informational

Tabelle 39: RAID-Adapter-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
rtPredictiveFailures Exceeded	9016	Adapter-**%d**, Kanal-**%d**, Ziel-**%d**: Vorhersehbarer Fehler wurde protokolliert. Zeichenfolge für Laufwerkidentifizierung = **%s** Prüfschlüssel = **0x%x**, ASC =**0x%x**, ASCQ = **0x%x**.	informational
rtPredictiveFailures False	9017	Adapter-**%d**, Kanal-**%d**, Ziel-**%d**: Schwellwert für Protokollierung vorhersehbarer Fehler wurde überschritten: [**FALSE**]. Zeichenfolge für Laufwerkidentifizierung = **%s** Prüfschlüssel = **0x%x**, ASC =**0x%x**, ASCQ = **0x%x**.	informational
rtReconstruction Completed	9014	Adapter-**%d**, Logisches Laufwerk-**%d**: Wiederherstellung erfolgreich abgeschlossen.	informational
rtReconstructionFailed	9015	Adapter-**%d**, Logisches Laufwerk-**%d**: Wiederherstellung gescheitert.	informational
rtReconstruction Started	9013	Adapter-**%d**, Logisches Laufwerk-**%d**: Wiederherstellung gestartet.	informational

Tabelle 39: RAID-Adapter-Traps

5.3.16 RomPilot-Traps (Rompilot.mib)

MIB-OID: 1.3.6.1.4.1.2487

Im Folgenden finden Sie eine alphabetische Übersicht über die RomPilot-Traps.

Trap-Name	ID	Bedeutung	Fehlerklasse
RomPilotColdReset	258	Phoenix RomPilot wurde nach dem Zurücksetzen des Systems geladen.	informational
RomPilot DiagnosticReset	259	Phoenix RomPilot wurde nach dem Zurücksetzen des Systems aus Diagnosegründen geladen.	informational
RomPilotFatalError	769	Phoenix RomPilot hat einen schwerwiegenden Fehler festgestellt.	informational
RomPilotGenericBoot	512	Phoenix RomPilot kündigt einen generischen Boot-Vorgang an (Betriebssystem wird geladen).	informational
RomPilotIDEBootReset	260	Phoenix RomPilot wurde nach dem Zurücksetzen des Systems (IDE-Boot-Vorgang) geladen.	informational
RomPilotOSStarted	1280	Phoenix RomPilot kündigt an, dass das Betriebssystem gestartet wurde.	informational
RomPilot PostWarningError	771	Phoenix RomPilot hat eine Warnung während des POST festgestellt.	informational
RomPilotPressF1	770	Phoenix RomPilot läuft. Zum Fortsetzen des Vorgangs muss die Taste F1 gedrückt werden.	informational

Tabelle 40: RomPilot-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
RomPilot UnspecifiedReset	256	Phoenix RomPilot wurde nach einem nicht angegebenen Zurücksetzen des Systems (vermutlich Ausschalten) geladen.	informational
RomPilotWarmReset	257	Phoenix RomPilot wurde nach einem Warmstart des Systems geladen.	informational

Tabelle 40: RomPilot-Traps

5.3.17 ServerControl-Traps (SC.mib)

MIB-OID: 1.3.6.1.4.1.231.2.10.2

Im Folgenden finden Sie eine alphabetische Übersicht über die ServerControl-Traps.

Trap-Name	ID	Bedeutung	Fehlerklasse
cabinetNotConfigured	623	Anlage ist nicht konfiguriert.	informational
cabinetSwitchedOff	617	Anlage wurde ausgeschaltet.	informational
cabinetSwitchedOn	618	Anlage wurde eingeschaltet.	informational
correctableMemError	643	Behebbarer Speicherfehler.	minor
correctableMemError Addr	637	Behebbarer Speicherfehler bei **address**.	minor
correctableMemError Bank	639	Behebbarer Speicherfehler bei **bank**.	minor
correctableMemError Module	641	Behebbarer Speicherfehler bei **module**.	minor
fanCriticalError	622	Ein Ventilator befindet sich in einem kritischen Zustand und wird demnächst ausfallen.	informational
fanError	601	Ventilator ist ausgefallen.	critical
fanOk	629	Ventilator ist in Ordnung.	informational
frontDoorStatusChanged	646	Status der vorderen Klappe hat sich geändert.	informational
housingOpenStatus Changed	647	Status des Gehäuses hat sich geändert.	informational
internalError	620	Interner Fehler in der Software für die Server Management-Steuereinheit.	informational

Tabelle 41: ServerControl-Traps (SC.mib)

Trap-Name	ID	Bedeutung	Fehlerklasse
memErrorModuleFailing	669	Ein Speichermodul ist fehlerhaft.	major
memErrorModule Prefailure	668	Für ein Speichermodul ist ein Fehler vorhersehbar.	major
memErrorModule Replaced	670	Ein fehlerhaftes Speichermodul wurde durch ein Hot-spare-Modul ersetzt.	major
notEnoughCabinets	615	Die tatsächliche Anzahl der Speichererweiterungen ist niedriger als in der Konfiguration angegeben.	major
powerOffTimeReached	645	Die Ausschaltzeit ist erreicht.	informational
powerSupplyAdded	625	Ein Netzteil wurde hinzugefügt.	informational
powerSupplyFailed	626	Ein Netzteil ist ausgefallen.	major
powerSupplyOk	627	Netzteil arbeitet wieder.	informational
powerSupplyRemoved	624	Netzteil wurde entfernt.	informational
powerSupplyStatus Critical	628	Zu wenig arbeitende Netzteile.	critical
scbBBUNotdetected	614	BBU ist zwar konfiguriert, lässt sich aber nicht ermitteln.	informational
scbUnconfiguredBBU Detected	613	BBU wurde zwar ermittelt, ist aber nicht konfiguriert.	informational
scbUnconfiguredUPS Detected	611	Eine unterbrechungsfreie Stromversorgung (USV) wurde zwar ermittelt, ist jedoch nicht konfiguriert.	informational

Tabelle 41: ServerControl-Traps (SC.mib)

Trap-Name	ID	Bedeutung	Fehlerklasse
scbUPSNotdetected	612	Eine unterbrechungsfreie Stromversorgung (USV) wurde zwar konfiguriert, ließ sich jedoch nicht ermitteln.	major
selftestError	609	Die Server Management-Steuereinheit ist ausgefallen.	critical
selftestWarning	608	Die Server Management-Steuereinheit hat während des Selbsttests ein untergeordnetes Problem festgestellt.	minor
serverManagement Disabled	631	Das Server Management-BIOS ist inaktiviert.	informational
serverShutdown	621	Der Server wurde heruntergefahren.	informational
sieScBootCountZero	666	Beim Hochfahren steht der Boot-Wiederholungszähler auf Null.	major
sieScBootError	661	Es kann kein bootfähiges Betriebssystem gefunden werden.	informational
sieScBootWatchdogExpired	662	Der Boot Watchdog ist abgelaufen.	informational
sieScCpuPrefailure	673	Ein CPU-Fehler ist vorhersehbar.	major
sieScDiagnosticBoot	665	Der Server wurde zurückgesetzt, Diagnostic-Boot ist aktiv.	informational
sieScMessageLogFull	667	System Event-Log ist voll. Meldungen können nicht mehr protokolliert werden. Der Trap erscheint nicht für Wraparound-Protokolle.	minor

Tabelle 41: ServerControl-Traps (SC.mib)

Trap-Name	ID	Bedeutung	Fehlerklasse
sieScMessageLog Warning	672	Der Grenzwert für die Anzahl der Einträge im System EventLog wurde überschritten.	minor
sieScNoBootCpu	658	Der Systemboot schlug fehl, weil keine gültige Boot CPU gefunden wurde.	informational
sieScPostError	659	Der Systemboot schlug fehl, weil der Power on-Selbsttest (POST) einen Fehler angezeigt hat.	informational
sieScPowerFail	674	Ausfall der Gleichspannung im angegebenen Schrank. Das System steht, wenn dieses Ereignis auftritt.	critical
sieScPowerOn	657	Der Server wurde eingeschaltet.	informational
sieScSetupEntered	660	Der BIOS Setup wurde eingetragen.	informational
sieScSoftwareWatchdog Expired	663	Der Software Watchdog ist abgelaufen.	informational
sieScUserAuthentication Failure	664	Eine fehlerhafte Benutzer-Authentifizierung wurde von PPP, FTP, HTTP oder Telnet registriert.	major
sniScCpuSpeedChanged	656	CPU-Geschwindigkeit hat sich wegen Temperaturproblemen verändert.	informational
sniScFanAdded	653	Der angegebene Hot-Plug-Lüfter wurde eingefügt.	informational
sniScFanRemoved	654	Der angegebene Hot-Plug-Lüfter wurde entfernt.	informational

Tabelle 41: ServerControl-Traps (SC.mib)

Trap-Name	ID	Bedeutung	Fehlerklasse
sniScPowerSupply RedundancyLost	671	Redundante Stromversorgung ist nicht verfügbar.	minor
sniScRedundant FanFailed	648	Der angegebene redundante Lüfter ist defekt.	major
sniScRedundant PowerSupplyFailed	649	Ein redundantes Hot-Replace-Netzteil ist defekt.	major
sniScShutdown Cancelled	655	Ein anstehender Systemabschluss des Servers wurde vom Benutzer abgebrochen.	informational
sniScVoltageOk	650	Die Spannung des Netzteils liegt wieder im normalen Bereich.	informational
sniScVoltageTooHigh	652	Die Spannung des Netzteils ist zu hoch.	critical
sniScVoltageTooLow	651	Die Spannung des Netzteils ist zu niedrig.	critical
svCommunication Established	636	Verbindung zur Server Management-Steuereinheit wurde hergestellt.	informational
svCommunicationFailure	610	Verbindung zur Server Management-Steuereinheit wurde unterbrochen.	critical
tempCritical	604	Die Temperatur hat ein kritisches Niveau erreicht.	critical
tempOk	602	Die Temperatur befindet sich im normalen Bereich.	informational
tempSensorBroken	630	Der Temperaturfühler ist defekt oder nicht angeschlossen.	major
tempSensorOk	635	Der Temperaturfühler arbeitet wieder.	informational

Tabelle 41: ServerControl-Traps (SC.mib)

Trap-Name	ID	Bedeutung	Fehlerklasse
tempWarn	603	Die Temperatur hat die Warnstufe erreicht.	major
testTrap	600	Test-Trap zum Prüfen der Trap-Verbindung.	informational
tooManyCabinets	616	Die tatsächliche Anzahl der Speicher-Subsysteme ist höher als in der Konfiguration angegeben.	minor
trapAcFail	632	Stromversorgung ist ausgefallen.	critical
trapDuplicateCabinetId	633	Zwei oder mehr Anlagen (Server oder Speicher-Subsysteme) weisen dieselbe ID auf.	major
trapEventLog	634	Ein Fehler wurde aufgezeichnet. Nähere Informationen finden Sie im Ereignis-/Fehlerprotokoll (Wiederherstellung) für die Serververwaltung. Dieser Fehler könnte aufgetreten sein, da vor dem Ausführen des Agenten ein Fehler aufgetreten ist, bzw. auf Grund eines anderen Fehlers ohne einen bestimmten Trap.	major

Tabelle 41: ServerControl-Traps (SC.mib)

Trap-Name	ID	Bedeutung	Fehlerklasse
trapOnBattery	606	Stromausfall. Anlage wird mit Batteriestrom betrieben. Die USV arbeitet mit Batteriestrom oder das Netzteil wird über die Ersatzbatterieeinheit (BBU, Battery Backup Unit) mit Strom versorgt. Dieser Trap ist dauerhaft und wird im Abstand von einer Minute solange gesendet, bis die Stromversorgung wiederhergestellt ist oder das System ausgeschaltet wird.	critical
trapOnMains	607	Stromversorgung ist in Ordnung.	informational
uncorrectableMemError	644	Nicht behebbarer Speicherfehler.	critical
uncorrectableMem ErrorAddr	638	Nicht behebbarer Speicherfehler bei **address**.	critical
uncorrectableMemError Bank	640	Nicht behebbarer Speicherfehler bei **bank**.	critical
uncorrectableMemError Module	642	Nicht behebbarer Speicherfehler bei **module**.	critical

Tabelle 41: ServerControl-Traps (SC.mib)

5.3.18 ServerControl-Traps (SC2.mib)

MIB-OID: 1.3.6.1.4.1.231.2.10.2.2.10.20

Im Folgenden finden Sie eine alphabetische Übersicht über die ServerControl-Traps.

Trap-Name	ID	Bedeutung	Fehlerklasse
sc2TrapAcFail	2040	Netzausfall im angegebenen Schrank. Dieser Trap tritt nur in Storage-Extension-Schränken ohne USV oder BBU auf. Ein Server hat keine Zeit, diesen Trap zu senden.	critical
sc2TrapBatteryVoltage Prefail	2054	Die Batterie wird ausfallen.	major
sc2TrapBiosSelftest Error	2005	Ein kritischer Fehler ist beim BIOS-Selbsttest aufgetreten. Dieser Fehler muss beachtet werden, um die Fehlerbedingung zu klären.	critical
sc2TrapBootMessage LogEntry	2102	Eine Fehlermeldung wurde in die Fehlerdatei des Systemboards geschrieben. Das geschieht, wenn eine Fehler auftritt ohne einen bestimmten Trap oder bevor die SNMP-Agenten laufen. Nähere Informationen finden Sie in Fehlerprotokoll des Server Managements.	major
sc2TrapBootRetryCount Zero	2095	Beim Hochfahren steht der Boot-Wiederholungszähler auf Null.	major

Tabelle 42: ServerControl-Traps (SC2.mib)

Trap-Name	ID	Bedeutung	Fehlerklasse
sc2TrapCabinetSwitchedOff	2090	Dieser Trap wird gesendet, wenn ein Schrank abgeschaltet ist. Dieser Trap kann aus offensichtlichen Gründen nicht gesendet werden, wenn der Hauptschrank abgeschaltet ist.	informational
sc2TrapCabinetSwitchedOn	2091	Dieser Trap wird gesendet, wenn ein Schrank eingeschaltet ist.	informational
sc2TrapCommunicationEstablished	2002	Verbindung mit der Server Management Steuereinheit wurde wieder hergestellt.	informational
sc2TrapCommunicationFailure	2001	Verbindung mit der Server Management Steuereinheit wurde unterbrochen.	minor
sc2TrapControllerSelftestError	2004	Fehler beim Selbsttest der Steuereinheit.	critical
sc2TrapControllerSelftestWarning	2003	Warnung beim Selbsttest der Steuereinheit.	minor
sc2TrapCorrectableMemErrorAddr	2060	Behebbarer Speicherfehler an der angegebenen Adresse.	informational
sc2TrapCorrectableMemErrorBank	2062	Behebbarer Speicherfehler auf der angegebenen Speicherbank.	informational
sc2TrapCorrectableMemErrorModule	2064	Behebbarer Speicherfehler im angegebenen Speichermodul.	informational
sc2TrapCorrectableMemError	2066	Behebbarer Speicherfehler an einer unbekannten Stelle.	informational
sc2TrapCpuPrefail	2081	Ein CPU-Fehler ist vorhersehbar.	major

Tabelle 42: ServerControl-Traps (SC2.mib)

Trap-Name	ID	Bedeutung	Fehlerklasse
sc2TrapCpuSpeedChanged	2080	Wegen eines Temperaturproblems wurde die Geschwindigkeit des Prozessors geändert.	informational
sc2TrapDcFail	2041	Ausfall der Gleichspannung im angegebenen Schrank. Dies ist das Ergebnis der Systemspannungssensor-Überwachung. System steht, wenn dieser Fehler auftritt.	critical
sc2TrapFanAdded	2010	Der angegebene Hot-Plug-Lüfter wurde eingefügt.	informational
sc2TrapFanCritical	2013	Angegebener Lüfter ist kritisch.	major
sc2TrapFanFailed	2014	Angegebener Lüfter ist ausgefallen.	critical
sc2TrapFanOk	2012	Angegebener Lüfter läuft wieder.	informational
sc2TrapFanRemoved	2011	Der angegebene Hot-Plug-Lüfter wurde entfernt.	informational
sc2TrapIntrusionAssertion	2110	Tür oder Gehäuse ist offen.	major
sc2TrapIntrusionChanged	2112	Tür oder Gehäuse wurde geöffnet oder geschlossen.	major
sc2TrapIntrusionDeassertion	2111	Tür oder Gehäuse wurde geschlossen.	informational
sc2TrapMemErrorModuleFailing	2069	Speichermodul ist ausgefallen.	major
sc2TrapMemErrorModulePrefail	2068	Für ein Speichermodul ist ein Fehler vorhersehbar.	major

Tabelle 42: ServerControl-Traps (SC2.mib)

Trap-Name	ID	Bedeutung	Fehlerklasse
sc2TrapMemErrorModuleReplaced	2070	Ein Speichermodul ist ausgefallen und wurde durch das Hot-spare-Module ersetzt.	major
sc2TrapMessageLogFull	2100	System Event-Log ist voll. Meldungen können nicht mehr protokolliert werden. Diesen Trap gibt es für Wraparound-Logs nicht.	minor
sc2TrapMessageLogWarning	2101	Der Grenzwert für die Anzahl der Einträge im System EventLog wurde überschritten.	minor
sc2TrapOnBattery	2042	Die USV arbeitet mit Batteriestrom oder das Netzteil wird über die Ersatzbatterieeinheit (BBU, Battery Backup Unit) mit Strom versorgt. Dieser Trap ist dauerhaft und wird im Abstand von einer Minute solange gesendet, bis die Stromversorgung wiederhergestellt ist oder das System ausgeschaltet wird.	critical
sc2TrapOnMains	2043	Die Stromversorgung ist nach einem Stromausfall wieder in Ordnung.	informational
sc2TrapPowerOffTimeReached	2092	Ausschaltzeit wurde erreicht.	informational
sc2TrapPowerSupplyAdded	2030	Hot-Replace-Netzteil wurde hinzugefügt.	informational
sc2TrapPowerSupplyCritical	2033	Status des Netzteils ist kritisch.	critical

Tabelle 42: ServerControl-Traps (SC2.mib)

Trap-Name	ID	Bedeutung	Fehlerklasse
sc2TrapPowerSupplyFailed	2034	Hot-Replace-Netzteil ist ausgefallen.	major
sc2TrapPowerSupplyOk	2032	Netzteil arbeitet wieder.	informational
sc2TrapPowerSupplyRedundancyLost	2036	Redundante Stromversorgung ist nicht verfügbar.	minor
sc2TrapPowerSupplyRemoved	2031	Hot-Replace-Netzteil wurde entfernt.	informational
sc2TrapRedundantFanFailed	2015	Der angegebene redundante Lüfter ist defekt.	major
sc2TrapRedundantPowerSupplyFailed	2035	Ein redundantes Hot-Replace-Netzteil ist defekt.	major
sc2TrapServerShutdown	2093	Server wird heruntergefahren.	informational
sc2TrapSevereSystemError	2006	Neustart des Systems nach einem Serverproblem. Nähere Informationen in der Server Management Meldungsdatei (Recovery Log).	critical
sc2TrapShutdownCancelled	2094	Anstehender Server-Shutdown wurde abgebrochen.	informational
sc2TrapTempCritical	2022	Temperaturanzeige ist außerhalb des Toleranzbereichs. Das System wird heruntergefahren und ausgeschaltet.	critical
sc2TrapTempOk	2020	Temperaturanzeige hat ein normales Niveau erreicht.	informational
sc2TrapTempSensorOk	2023	Defekter Temperaturfühler ist wieder in Ordnung.	informational

Tabelle 42: ServerControl-Traps (SC2.mib)

Trap-Name	ID	Bedeutung	Fehlerklasse
sc2TrapTempSensorBroken	2024	Temperaturfühler ist defekt.	major
sc2TrapTempWarning	2021	Temperaturanzeige hat die Warnstufe erreicht.	major
sc2TrapTest	2000	Test-Trap zur Verbindungsprüfung.	informational
sc2TrapUncorrectableMemError	2067	Nicht behebbarer Speicherfehler an unbekannter Stelle.	critical
sc2TrapUncorrectableMemErrorAddr	2061	Nicht behebbarer Speicherfehler an der angegebenen Adresse.	critical
sc2TrapUncorrectableMemErrorBank	2063	Nicht behebbarer Speicherfehler auf der angegebenen Speicherbank.	critical
sc2TrapUncorrectableMemErrorModule	2065	Behebbarer Speicherfehler im angegebenen Speichermodul.	critical
sc2TrapVoltageOk	2050	Die Spannung des Netzteils liegt wieder im normalen Bereich.	informational
sc2TrapVoltageFailed	2053	Spannung am Netzteil liegt außerhalb des normalen Bereichs.	critical
sc2TrapVoltageTooHigh	2052	Die Spannung des Netzteils ist zu hoch.	critical
sc2TrapVoltageTooLow	2051	Die Spannung des Netzteils ist zu niedrig.	critical
sc2TrapDrvMonEventMessage	2150	Der Driver Monitor hat ein Ereignis der Fehlerklasse „informational“ festgestellt.	informational

Tabelle 42: ServerControl-Traps (SC2.mib)

Trap-Name	ID	Bedeutung	Fehlerklasse
sc2TrapDrvMonEventWarning	2151	Der Driver Monitor hat ein Ereignis der Fehlerklasse „warning“ festgestellt.	minor
sc2TrapDrvMonEventError	2152	Der Driver Monitor hat ein Ereignis der Fehlerklasse „error“ festgestellt.	major

Tabelle 42: ServerControl-Traps (SC2.mib)

5.3.19 ServerView-Traps (ServerView.mib)

MIB-OID: 1.3.6.1.4.1.231.2.10.2

Im Folgenden finden Sie eine alphabetische Übersicht über die ServerView-Traps.

Trap-Name	ID	Bedeutung	Fehlerklasse
sniSvGenericTrap Forward	700	ServerView-Alarmsignal empfangen.	informational
sniSvPagerOff	701	Pager sollte ausgeschaltet werden.	informational
sniSvPassThrough TrapForward	703	Wird weitergeleitet, wenn der Event Manager einen Trap empfängt, der weitergeleitet werden soll. Der ursprüngliche Server-Name und der Dringlichkeitsgrad werden beibehalten.	informational
sniSvServerState Changed	702	Wird vom Operations Manager generiert, wenn sich der Status des Servers ändert (verwaltbar/nicht verwaltbar).	informational

Tabelle 43: ServerView-Traps

5.3.20 ServerView-Status-Trap (Status.mib)

MIB-OID: 1.3.6.1.4.1.231.2.10.2

Im Folgenden finden Sie eine Beschreibung des ServerView-Status-Traps.

Trap-Name	ID	Bedeutung	Fehlerklasse
sieStTrapStatusChanged	1100	Der System-Status am Server hat sich verändert.	informational

Tabelle 44: ServerView-Status-Trap

5.3.21 Bandlaufwerke-Traps (tapealrt.mib)

MIB-OID: 1.3.6.1.4.1.11.2.3.9.7.1

Im Folgenden finden Sie eine alphabetische Übersicht über die Bandlaufwerk-Traps.

Trap-Name	ID	Bedeutung	Fehlerklasse
tapeAlertTrap1	1	Das Bandlaufwerk kann keine Daten lesen. Es sind keine Daten verloren gegangen, es ist jedoch zu einem Leistungsabfall des Bandlaufwerks gekommen.	minor
tapeAlertTrap2	2	Das Bandlaufwerk kann keine Daten schreiben. Es sind keine Daten verloren gegangen, die Speicherkapazität des Bandlaufwerks ist jedoch geringer geworden.	minor
tapeAlertTrap3	3	Der Vorgang wurde gestoppt, da beim Lesen oder Schreiben von Daten ein Fehler aufgetreten ist, den das Laufwerk nicht beheben kann.	minor
tapeAlertTrap4	4	Ihre Daten sind gefährdet: 1. Kopieren Sie alle erforderlichen Daten von diesem Band. 2. Verwenden Sie dieses Band nicht mehr. 3. Starten Sie den Vorgang mit einem anderen Band erneut.	critical

Tabelle 45: Traps für Bandlaufwerke

Trap-Name	ID	Bedeutung	Fehlerklasse
tapeAlertTrap5	5	Das Band ist beschädigt oder das Laufwerk weist einen Fehler auf. Wenden Sie sich an den Hersteller des Bandlaufwerks.	critical
tapeAlertTrap6	6	Das Band stammt aus einem fehlerhaften Bestand oder das Bandlaufwerk weist einen Fehler auf: 1. Verwenden Sie ein einwandfreies Band zum Testen des Laufwerks. 2. Wenn der Fehler weiterhin auftritt, wenden Sie sich an den Hersteller des Bandlaufwerks.	critical
tapeAlertTrap7	7	Die Lebensdauer der Bandkassette ist nahezu erschöpft: 1. Kopieren Sie alle erforderlichen Daten auf ein anderes Band. 2. Vernichten Sie das alte Band.	minor
tapeAlertTrap8	8	Die Bandkassette kann keine Daten speichern. Alle Daten, die Sie auf dieser Kassette speichern, könnten verloren gehen. Ersetzen Sie die Kassette durch eine funktionierende Bandkassette.	minor

Tabelle 45: Traps für Bandlaufwerke

Trap-Name	ID	Bedeutung	Fehlerklasse
tapeAlertTrap9	9	Sie versuchen, Daten auf eine schreibgeschützte Bandkassette zu schreiben. Entfernen Sie die schreibgeschützte Kassette oder verwenden Sie ein anderes Band.	critical
tapeAlertTrap10	10	Sie können die Kassette nicht entnehmen, da das Bandlaufwerk in Gebrauch ist. Warten Sie, bis der Vorgang abgeschlossen ist, bevor Sie die Kassette entnehmen.	informational
tapeAlertTrap11	11	Bei dem Band im Laufwerk handelt es sich um eine Reinigungskassette. Wenn Sie Daten sichern oder wiederherstellen möchten, legen Sie ein Datenband ein.	informational
tapeAlertTrap12	12	Sie haben versucht, einen Kassettentyp einzulegen, der nicht von diesem Laufwerk unterstützt wird.	informational
tapeAlertTrap13	13	Der Vorgang ist gescheitert, da bei dem Band im Laufwerk ein Fehler aufgetreten ist: 1. Vernichten Sie das alte Band. 2. Starten Sie den Vorgang mit einem anderen Band erneut.	critical

Tabelle 45: Traps für Bandlaufwerke

Trap-Name	ID	Bedeutung	Fehlerklasse
tapeAlertTrap14	14	Der Vorgang ist gescheitert, da bei dem Band im Laufwerk ein Fehler aufgetreten ist: 1. Versuchen Sie nicht, die Bandkassette zu entnehmen. 2. Wenden Sie sich an den Hersteller des Bandlaufwerks.	critical
tapeAlertTrap15	15	Der Speicher auf der Bandkassette weist einen Fehler auf. Verwenden Sie dieses Band nicht mehr für Sicherungsvorgänge.	minor
tapeAlertTrap16	16	Der Vorgang ist fehlgeschlagen, da die Bandkassette manuell entnommen wurde, während auf das Bandlaufwerk Daten geschrieben oder vom Laufwerk gelesen wurden.	critical
tapeAlertTrap17	17	Sie haben eine Kassette eingelegt, die auf diesem Laufwerk lediglich für Nur-Lese-Vorgänge eingesetzt werden kann. Die Kassette wird als schreibgeschützte Kassette angezeigt.	minor
tapeAlertTrap18	18	Das Verzeichnis auf der Bandkassette wurde beschädigt. Dies führt zu Leistungseinbußen bei der Dateisuche.	minor

Tabelle 45: Traps für Bandlaufwerke

Trap-Name	ID	Bedeutung	Fehlerklasse
tapeAlertTrap19	19	Die Lebensdauer der Bandkassette ist nahezu erschöpft. Es empfiehlt sich Folgendes: 1. Verwenden Sie für den nächsten Sicherungsvorgang eine andere Bandkassette. 2. Bewahren Sie diese Bandkassette gut auf, falls Sie von diesem Band zu einem späteren Zeitpunkt Daten wiederherstellen müssen.	informational
tapeAlertTrap20	20	Das Bandlaufwerk muss gereinigt werden: 1. Entnehmen Sie das Band, sobald der Vorgang gestoppt wurde, und reinigen Sie das Laufwerk. 2. Falls der Vorgang noch nicht abgeschlossen ist, warten Sie, bis dies der Fall ist, und reinigen Sie anschließend das Laufwerk.	critical

Tabelle 45: Traps für Bandlaufwerke

Trap-Name	ID	Bedeutung	Fehlerklasse
tapeAlertTrap21	21	Das Bandlaufwerk muss routinemäßig gereinigt werden: 1. Warten Sie, bis der aktuelle Vorgang abgeschlossen ist. 2. Verwenden Sie anschließend eine Reinigungskassette.	minor
tapeAlertTrap22	22	Die letzte in diesem Bandlaufwerk verwendete Reinigungskassette ist verbraucht: 1. Vernichten Sie die verbrauchte Reinigungskassette. 2. Warten Sie, bis der aktuelle Vorgang abgeschlossen ist. 3. Verwenden Sie anschließend eine neue Reinigungskassette.	critical

Tabelle 45: Traps für Bandlaufwerke

Trap-Name	ID	Bedeutung	Fehlerklasse
tapeAlertTrap23	23	Die zuletzt für das Bandlaufwerk verwendete Reinigungskassette wies einen ungültigen Typ auf: 1. Verwenden Sie diese Reinigungskassette nicht für dieses Laufwerk. 2. Warten Sie, bis der aktuelle Vorgang abgeschlossen ist. 3. Verwenden Sie anschließend eine geeignete Reinigungskassette.	critical
tapeAlertTrap29	29	Es ist eine vorsorgliche Wartung des Bandlaufwerks erforderlich. Prüfen Sie, ob im Handbuch zum Bandlaufwerk einheitenspezifische Anweisungen zu Wartungsvorgängen enthalten sind oder wenden Sie sich an den Hersteller des Bandlaufwerks.	minor
tapeAlertTrap30	30	Das Bandlaufwerk weist einen Hardwarefehler auf: 1. Entnehmen Sie das Band oder Magazin. 2. Setzen Sie das Laufwerk zurück. 3. Starten Sie den Vorgang erneut.	critical

Tabelle 45: Traps für Bandlaufwerke

Trap-Name	ID	Bedeutung	Fehlerklasse
tapeAlertTrap31	31	Das Bandlaufwerk weist einen Hardwarefehler auf: 1. Schalten Sie das Bandlaufwerk aus und wieder ein. 2. Starten Sie den Vorgang erneut. 3. Wenn der Fehler weiterhin auftritt, wenden Sie sich an den Hersteller des Bandlaufwerks.	critical
tapeAlertTrap32	32	Das Bandlaufwerk weist einen Fehler bei der Host-Schnittstelle auf: 1. Überprüfen Sie die Kabel und Kabelverbindungen. 2. Starten Sie den Vorgang erneut.	minor
tapeAlertTrap33	33	Der Vorgang ist gescheitert: 1. Entnehmen Sie das Band oder Magazin. 2. Legen Sie das Band oder Magazin erneut ein. 3. Starten Sie den Vorgang erneut.	critical

Tabelle 45: Traps für Bandlaufwerke

Trap-Name	ID	Bedeutung	Fehlerklasse
tapeAlertTrap34	34	Das Herunterladen der Firmware ist gescheitert, da Sie versucht haben, die falsche Firmware für dieses Bandlaufwerk zu verwenden. Besorgen Sie die richtige Firmware und führen Sie den Vorgang erneut aus.	minor
tapeAlertTrap35	35	Die Umgebungsbedingungen im Bandarchiv haben den maximalen Feuchtigkeitswert überschritten.	minor
tapeAlertTrap36	36	Die allgemeinen Umgebungsbedingungen im Bandarchiv haben die maximale Temperatur überschritten.	minor
tapeAlertTrap37	37	Die Spannungsversorgung zum Bandlaufwerk liegt über den angegebenen Spezifikationen.	minor
tapeAlertTrap38	38	Es wird ein Hardwarefehler am Bandlaufwerk vorhergesagt. Wenden Sie sich an den Hersteller des Bandlaufwerks.	critical

Tabelle 45: Traps für Bandlaufwerke

Trap-Name	ID	Bedeutung	Fehlerklasse
tapeAlertTrap39	39	Am Bandlaufwerk liegt möglicherweise ein Hardwarefehler vor. Führen Sie die erweiterten Diagnoseprogramme aus, um den Fehler zu überprüfen und festzustellen. Prüfen Sie, ob im Handbuch zum Bandlaufwerk einheitenspezifische Anweisungen zum Ausführen erweiterter Diagnosetests enthalten sind.	minor
tapeAlertTrap40	40	Der Bandwechsler kann nicht mit dem Bandlaufwerk kommunizieren: 1. Schalten Sie das automatische Bandladegerät aus und wieder ein. 2. Starten Sie den Vorgang erneut. 3. Wenn der Fehler weiterhin auftritt, wenden Sie sich an den Hersteller des Bandlaufwerks.	critical

Tabelle 45: Traps für Bandlaufwerke

Trap-Name	ID	Bedeutung	Fehlerklasse
tapeAlertTrap41	41	Aufgrund eines vorangegangenen Hardwarefehlers ist ein Band im automatischen Bandladegerät geblieben: 1. Legen Sie ein leeres Magazin ein, um den Fehler zu beheben. 2. Wenn der Fehler damit nicht behoben ist, schalten Sie das automatische Bandladegerät aus und wieder ein. 3. Wenn der Fehler weiterhin auftritt, wenden Sie sich an den Hersteller des Bandlaufwerks.	critical
tapeAlertTrap42	42	Am automatischen Bandladegerät ist ein Fehler aufgetreten.	minor

Tabelle 45: Traps für Bandlaufwerke

Trap-Name	ID	Bedeutung	Fehlerklasse
tapeAlertTrap43	43	Der Vorgang ist gescheitert, da die Klappe des automatischen Bandladegeräts geöffnet ist: 1. Entfernen Sie alle Hindernisse an der Klappe des automatischen Bandladegeräts. 2. Entnehmen Sie das Magazin und legen Sie es erneut ein. 3. Wenn der Fehler damit nicht behoben ist, schalten Sie das automatische Bandladegerät aus und wieder ein. 4. Wenn der Fehler weiterhin auftritt, wenden Sie sich an den Hersteller des Bandlaufwerks.	critical

Tabelle 45: Traps für Bandlaufwerke

Trap-Name	ID	Bedeutung	Fehlerklasse
tapeAlertTrap44	44	Das automatische Bandladegerät weist einen Hardwarefehler auf: 1. Schalten Sie das automatische Bandladegerät aus und wieder ein. 2. Starten Sie den Vorgang erneut. 3. Wenn der Fehler weiterhin auftritt, wenden Sie sich an den Hersteller des Bandlaufwerks.	critical
tapeAlertTrap45	45	Das automatische Bandladegerät kann nicht ohne Magazin verwendet werden. 1. Legen Sie das Magazin in das automatische Bandladegerät ein. 2. Starten Sie den Vorgang erneut.	critical
tapeAlertTrap46	46	Es wird ein Hardwarefehler am Bandwechsler vorhergesagt. Wenden Sie sich an den Hersteller des Bandlaufwerks.	minor

Tabelle 45: Traps für Bandlaufwerke

Trap-Name	ID	Bedeutung	Fehlerklasse
tapeAlertTrap256	256	Das Bandarchiv kann nicht mit dem Laufwerk kommunizieren: 1. Schalten Sie das Bandarchiv aus und wieder ein. 2. Starten Sie den Vorgang erneut. 3. Wenn der Fehler weiterhin auftritt, wenden Sie sich an den Hersteller des Bandarchivs.	critical
tapeAlertTrap257	257	Beim Bandarchiv ist ein Fehler aufgetreten. Wenn der Fehler weiterhin auftritt, wenden Sie sich an den Hersteller des Bandarchivs.	minor
tapeAlertTrap258	258	Das Bandarchiv weist einen Hardwarefehler auf: 1. Setzen Sie das Bandarchiv zurück. 2. Starten Sie den Vorgang erneut. Prüfen Sie, ob im Handbuch zum Bandarchiv einheitenspezifische Anweisungen zum Zurücksetzen der Einheit enthalten sind.	critical

Tabelle 45: Traps für Bandlaufwerke

Trap-Name	ID	Bedeutung	Fehlerklasse
tapeAlertTrap259	259	Das Bandarchiv weist einen Hardwarefehler auf: 1. Schalten Sie das Bandarchiv aus und wieder ein. 2. Starten Sie den Vorgang erneut. 3. Wenn der Fehler weiterhin auftritt, wenden Sie sich an den Hersteller des Bandarchivs. Prüfen Sie, ob im Handbuch zum Bandarchiv einheitenspezifische Anweisungen zum Ein- und Ausschalten der Einheit enthalten sind.	critical
tapeAlertTrap260	260	Das Bandarchiv weist möglicherweise einen Hardwarefehler auf. Führen Sie die erweiterten Diagnoseprogramme aus, um den Fehler zu überprüfen und festzustellen. Prüfen Sie, ob im Handbuch zum Bandarchiv einheitenspezifische Anweisungen zum Ausführen erweiterter Diagnosetests enthalten sind.	minor

Tabelle 45: Traps für Bandlaufwerke

Trap-Name	ID	Bedeutung	Fehlerklasse
tapeAlertTrap261	261	Das Bandarchiv weist einen Fehler bei der Host-Schnittstelle auf: 1. Überprüfen Sie die Kabel und Kabelverbindungen. 2. Starten Sie den Vorgang erneut.	critical
tapeAlertTrap262	262	Es wird ein Hardwarefehler des Bandarchivs vorhergesagt. Wenden Sie sich an den Hersteller des Bandarchivs.	minor
tapeAlertTrap263	263	Es ist eine vorsorgliche Wartung des Bandarchivs erforderlich. Prüfen Sie, ob im Handbuch zum Bandarchiv einheitenspezifische Anweisungen für Wartungsvorgänge enthalten sind, oder wenden Sie sich an den Hersteller des Bandarchivs.	minor
tapeAlertTrap264	264	Die allgemeinen Umgebungsbedingungen im Bandarchiv haben den maximalen Feuchtigkeitswert überschritten.	critical
tapeAlertTrap265	265	Die allgemeinen Umgebungsbedingungen im Bandarchiv haben die maximale Temperatur überschritten.	critical

Tabelle 45: Traps für Bandlaufwerke

Trap-Name	ID	Bedeutung	Fehlerklasse
tapeAlertTrap266	266	Die Spannungsversorgung zum Bandarchiv liegt über den angegebenen Spezifikationen. Es liegt ein potenzieller Fehler am Netzteil oder ein Ausfall eines redundanten Netzteils vor.	critical
tapeAlertTrap267	267	Aufgrund eines vorangegangenen Hardwarefehlers ist in einem Laufwerk innerhalb des Bandarchivs eine Kassette geblieben: 1. Legen Sie ein leeres Magazin ein, um den Fehler zu beheben. 2. Wenn der Fehler damit nicht behoben ist, schalten Sie das Bandarchiv aus und wieder ein. 3. Wenn der Fehler weiterhin auftritt, wenden Sie sich an den Hersteller des Bandarchivs.	critical
tapeAlertTrap268	268	An einem Laufwerk liegt ein möglicher Fehler vor, da Kassetten zu kurz ausgeworfen werden bzw. es kommt zu Fehlern beim Herausnehmen einer Kassette. Wenn der Fehler weiterhin auftritt, wenden Sie sich an den Hersteller des Bandarchivs.	minor

Tabelle 45: Traps für Bandlaufwerke

Trap-Name	ID	Bedeutung	Fehlerklasse
tapeAlertTrap269	269	Es liegt ein möglicher Fehler am Bandarchiv beim Zurückstellen einer Kassette vor. Wenn der Fehler weiterhin auftritt, wenden Sie sich an den Hersteller des Bandarchivs.	minor
tapeAlertTrap270	270	Es liegt ein möglicher Fehler an einem Laufwerk oder dem Bandarchiv beim Laden von Kassetten vor, oder es wird eine nicht kompatible Kassette verwendet.	minor
tapeAlertTrap271	271	Der Vorgang ist gescheitert, da die Klappe des Bandarchivs geöffnet ist: 1. Entfernen Sie alle Hindernisse an der Klappe des Bandarchivs. 2. Schließen Sie die Klappe des Bandarchivs. 3. Wenn der Fehler weiterhin auftritt, wenden Sie sich an den Hersteller des Bandarchivs.	critical
tapeAlertTrap272	272	Am Entnahme-/Eingabefach von Datenträgern im Bandarchiv liegt ein mechanischer Fehler vor.	critical

Tabelle 45: Traps für Bandlaufwerke

Trap-Name	ID	Bedeutung	Fehlerklasse
tapeAlertTrap273	273	Das Bandarchiv kann nicht ohne Magazin verwendet werden: 1. Legen Sie das Magazin in das Bandarchiv ein. 2. Starten Sie den Vorgang erneut.	critical
tapeAlertTrap274	274	Die Sicherheitsbestimmungen des Bandarchivs wurden verletzt.	minor
tapeAlertTrap275	275	Der Sicherheitsmodus des Bandarchivs wurde geändert. Das Bandarchiv wurde entweder in den sicheren Modus versetzt, oder das Bandarchiv hat diesen Modus verlassen.	informational
tapeAlertTrap276	276	Das Bandarchiv wurde manuell offline gesetzt und ist jetzt nicht mehr verfügbar.	informational
tapeAlertTrap277	277	Ein Laufwerk innerhalb des Bandarchivs wurde offline gesetzt.	informational
tapeAlertTrap278	278	Im Bandarchiv liegt ein möglicher Fehler an der Balkencode-Kennung oder der Scanner-Hardware vor. Wenn der Fehler weiterhin auftritt, wenden Sie sich an den Hersteller des Bandarchivs.	minor

Tabelle 45: Traps für Bandlaufwerke

Trap-Name	ID	Bedeutung	Fehlerklasse
tapeAlertTrap279	279	Das Bandarchiv hat eine Inkonsistenz in der Bestandsliste festgestellt. 1. Stellen Sie die Bestandsliste erneut zusammen, um die Inkonsistenz zu beheben. 2. Starten Sie den Vorgang erneut. Prüfen Sie, ob im Handbuch zum Bandarchiv spezielle Anweisungen zum Erstellen der Bestandsliste enthalten sind.	critical
tapeAlertTrap280	280	Es wurde versucht, einen Vorgang für das Bandarchiv durchzuführen, der derzeit nicht durchgeführt werden kann.	minor

Tabelle 45: Traps für Bandlaufwerke

5.3.22 Team-Server-Traps (Fujitsu)

Im Folgenden finden Sie eine Beschreibung der von den Fujitsu-Team-Servern gelieferten Traps.

Traps der ASM PRIVATE COMMIB (Asmpro.mib)

MIB-OID: 1.3.6.1.4.1.3764.3

Trap-Name	ID	Bedeutung	Fehlerklasse
trapACFail	13	Die Netz-Stromversorgung ist ausgefallen.	major
trapAssetChange	23	Die Ressourcen haben sich geändert.	major
trapBatteryFail	15	Die USV-Batterie ist ausgefallen.	major
trapBusUtilization	8	Die prozentuelle Bus-Auslastung übersteigt einen vorgegebenen Schwellwert.	major
trapBiosEventLog	20	Restart des BIOS-Eventlog hat neuen Event-Log.	major
trapBiosEventLog Utlization	21	Prozentuelle Nutzung des Eventlogs übersteigt einen vorgegebenen Schwellwert.	major
trapChassisIntrusion	16	Unbefugtes Öffnen des Server-Gehäuses.	major
trapCPUAbnormal	22	Interner Fehler der CPU.	major
trapCPUUtilization	7	Die prozentuelle CPU-Auslastung übersteigt einen vorgegebenen Schwellwert.	major
trapECC1BitError	3	Ein EEC-1-bit-Fehler ist aufgetreten.	major

Tabelle 46: ASM PRIVATE MIB traps

Trap-Name	ID	Bedeutung	Fehlerklasse
trapECCMBitError	4	Ein EEC-mehrfach-bit-Fehler ist aufgetreten.	critical
trapFanStop	5	Ein Ventilator ist ausgefallen.	major
trapFuseFail	17	Fehler der Schmelzsicherung.	major
trapMemoryUtilization	9	Die prozentuelle Speicherauslastung übersteigt einen vorgegebenen Schwellwert.	major
trapNICCounter	11	Ein NIC-Statistik-Zähler hat einen vorgegebenen Schwellwert überschritten.	major
trapPowerFanFail	14	Der Ventilator eines Stromversorgungs-Subsystems ist ausgefallen.	major
trapPSFail	12	Eine Stomversorgungseinheit ist ausgefallen.	major
trapRPSFail	18	Eine redundante Stromversorgungseinheit ist ausgefallen.	major
trapRPSFanFail	19	Der Ventilator einer redundanten Stromversorgungseinheit ist ausgefallen.	major
trapTemperatureCritical	2	Die Temperatur hat den Schwellwert der zweiten Stufe überschritten.	critical
trapVoltage	6	Die elektrische Spannung hat den sicheren Bereich überschritten.	major

Tabelle 46: ASM PRIVATE MIB traps

Trap-Name	ID	Bedeutung	Fehlerklasse
trapVolumeUtilization	10	Die Datenträgerauslastung hat einen Schwellwert überschritten.	major

Tabelle 46: ASM PRIVATE MIB traps

Traps der LDCM-MIB (Ldcm.mib)

MIB-OID: 1.3.6.1.4.1.343.2.5.1.2

Trap-Name	ID	Bedeutung	Fehlerklasse
ldcmCriticalTrap	5	Der Manager hat ein Ereignis der Fehlerklasse „critical“ gemeldet.	critical
ldcmFatalTrap	6	Der Manager hat ein Ereignis der Fehlerklasse „fatal“ gemeldet.	critical
ldcmInfoTrap	2	Der Manager hat ein Ereignis der Fehlerklasse „informational“ gemeldet.	informational
ldcmOkTrap	3	Der Manager hat ein Ereignis der Fehlerklasse „OK“ gemeldet.	informational
ldcmUnknownTrap	1	Der Manager hat ein unbekanntes Ereignis gemeldet.	informational
ldcmWarningTrap	4	Der Manager hat ein Ereignis der Fehlerklasse „warning“ gemeldet.	minor

Tabelle 47: Traps der LDCM-MIB

Traps der LDSM-MIB (Ldsm.mib)

MIB-OID: 1.3.6.1.4.1.343.2.5.1.3

Trap-Name	ID	Bedeutung	Fehlerklasse
ldsmCriticalTrap	4	Der Manager hat ein Ereignis der Fehlerklasse **critical** gemeldet.	critical
ldsmInformationalTrap	2	Der Manager hat ein Ereignis der Fehlerklasse **informational** gemeldet.	informational

Tabelle 48: Traps der LDSM-MIB

Trap-Name	ID	Bedeutung	Fehlerklasse
ldsmOkTrap	1	Der Manager hat ein Ereignis der Fehlerklasse **OK** gemeldet.	informational
ldsmWarningTrap	3	Der Manager hat ein Ereignis der Fehlerklasse **warning** gemeldet.	minor

Tabelle 48: Traps der LDSM-MIB

5.3.23 Threshold-Traps (Trap.mib)

MIB-OID: 1.3.6.1.4.1.231

Im Folgenden finden Sie eine alphabetische Übersicht über die Threshold-Traps.

Trap-Name	ID	Bedeutung	Fehlerklasse
sniInvDeltaTrap Underflow	131	DELTA-Schwellwert wurde unterschritten. Dieser Trap gibt an, dass eine der POLLVariablen nicht mehr in dem vom Benutzer angegebenen Intervall enthalten ist. Die Variable ist im Feld snilnvPollAlarm angegeben.	informational
sniInvPollDeltaExceed	130	DELTA-Schwellwert wurde überschritten. Dieser Trap gibt an, dass eine der POLLVariablen nicht mehr in dem vom Benutzer angegebenen Intervall enthalten ist. Die Variable ist im Feld snilnvPollAlarm angegeben.	informational

Tabelle 49: Threshold-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
sniInvPollTrapExceed	128	Schwellwert wurde überschritten. Dieser Trap gibt an, dass eine der POLLVariablen nicht mehr in dem vom Benutzer angegebenen Intervall enthalten ist. Die Variable ist im Feld snilnvPollAlarm angegeben.	informational
sniInvPollTrapUnderflow	129	Schwellwert wurde unterschritten. Dieser Trap gibt an, dass eine der POLLVariablen nicht mehr in dem vom Benutzer angegebenen Intervall enthalten ist. Die Variable ist im Feld snilnvPollAlarm angegeben.	informational
sniInvTrapInvalid	132	Schwellwert ist ungültig.	informational
sniInvTrapValid	133	Schwellwert ist gültig.	informational
sniNTAlert	304	Eine NT Alarmmeldung wurde in das Ereignisprotokoll geschrieben.	informational
sniNTChangeSecurity	302	Eine Sicherheitsänderung ist aufgetreten.	informational
sniNTChangeTime	305	Die Zeiteinstellung wurde geändert, eine uneinheitliche Zeitanpassung ist aufgetreten.	informational
sniNTDownServer	300	Server wird heruntergefahren.	informational
sniNTEventLogError	330	Ein Fehlereintrag wurde in das Ereignisprotokoll geschrieben.	informational

Tabelle 49: Threshold-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
sniNTEventLogFailure	334	Ein Eintrag für ein fehlerhaftes Ereignis wurde in das Ereignisprotokoll geschrieben.	informational
sniNTEventLog Information	332	Ein Informationseintrag wurde in das Ereignisprotokoll geschrieben.	informational
sniNTEventLogSuccess	333	Ein Eintrag für ein erfolgreiches Ereignis wurde in das Ereignisprotokoll geschrieben.	informational
sniNTEventLogWarning	331	Ein Warnungseintrag wurde in das Ereignisprotokoll geschrieben.	informational
sniNTFileChangeAttr	322	Datei- oder Verzeichniseigenschaften wurden geändert.	informational
sniNTFileChange DirName	321	Ein Verzeichnisname wurde geändert, erzeugt oder gelöscht.	informational
sniNTFileChangeLast Write	324	Die Zeit des letzten Schreibzugriffs für eine Datei wurde geändert.	informational
sniNTFileChangeName	320	Ein Dateiname wurde geändert, erzeugt oder gelöscht.	informational
sniNTFileChange Security	325	Die Sicherheitsmerkmale für eine Datei wurden geändert.	informational
sniNTFileChangeSize	323	Die Dateigröße wurde verändert.	informational
sniNTLoginUser	301	Ein Benutzer hat sich am Server angemeldet.	informational

Tabelle 49: Threshold-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
sniNTRegChangeAttr	311	In der Registry wurden die Attribute für einen Schlüssel oder sein Unterverzeichnis geändert.	informational
sniNTRegChangeLast Write	312	In der Registry wurde die Zeit des letzten Schreibzugriffs für einen Schlüssel oder sein Unterverzeichnis geändert.	informational
sniNTRegChangeName	310	In der Registry wurde ein Schlüsselname geändert.	informational
sniNTRegChange Security	313	In der Registry wurde das Sicherheitsmerkmal für einen Schlüssel oder sein Unterverzeichnis geändert.	informational
sniNTTrusteeChange	303	Für den Server wurde der Verwalter geändert.	informational
sniNWActivateScreen	014	Am Server wurde ein Bildschirm aktiviert.	informational
sniNWAlert	044	Eine Netware Alarmmeldung wurde an der Konsole ausgegeben.	informational
sniNWAllocate Connection	037	Am Server wurde eine Verbindung zugewiesen.	informational
sniNWChangeSecurity	013	Am Server erfolgte eine Sicherheitsänderung.	informational
sniNWChangeTime	051	Die Zeiteinstellung wurde geändert, eine uneinheitliche Zeitanpassung ist aufgetreten.	informational
sniNWClearConnection	009	Eine Verbindung wurde freigegeben.	informational
sniNWCloseFile	050	Eine Datei wurde geschlossen.	informational

Tabelle 49: Threshold-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
sniNWCloseScreen	021	Am Server wurde ein Bildschirm geschlossen.	informational
sniNWCreateBinderyObj	011	Ein Bindery-Object wurde erzeugt (NetWare).	informational
sniNWCreateObject	046	Für den Verzeichnis-Service (NetWare) wurde ein Objekt erzeugt.	informational
sniNWCreateProcess	028	Ein Prozess wurde erzeugt.	informational
sniNWDataMigration	041	Die Daten einer Datei wurden umgewandelt.	informational
sniNWDataDeMigration	042	Die Migration einer Datei wurde zurückgenommen.	informational
sniNWDeactivateScreen	018	Am Server wurde ein Bildschirm deaktiviert.	informational
sniNWDeleteBinderyObj	012	Ein Bindery-Object wurde gelöscht (NetWare).	informational
sniNWDeleteObject	047	Für den Verzeichnis-Service (NetWare) wurde ein Objekt gelöscht.	informational
sniNWDestroyProcess	029	Ein Prozess wurde beendet.	informational
sniNWDownServer	004	Server wird heruntergefahren.	critical
sniNWExitToDos	007	Server wechselt nach DOS.	critical
sniNWKeyWasPressed	017	Am Server wurde ein Schalter betätigt.	informational
sniNWLoginUser	010	Ein Benutzer hat sich am Server angemeldet.	informational
sniNWLogoutConnection	038	Ein Benutzer hat die Verbindung beendet.	informational
sniNWMLIDDeRegister	040	Ein Multiple Link Interface Treiber (MLID) wurde abgemeldet.	informational

Tabelle 49: Threshold-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
sniNWMLIDRegister	039	Ein Multiple Link Interface Treiber (MLID) wurde am Server angemeldet.	informational
sniNWModifyDirEntry	022	Am Server wurde ein Verzeichniseintrag geändert.	informational
sniNWModule Loaded	027	Ein Modul (z.B. NLM) wurde geladen.	informational
sniNWModuleUnloaded	009	Ein Modul (z.B. NLM) wurde entladen.	informational
sniNWNewPublic	032	Ein neues Public-Symbol wurde eingetragen.	informational
sniNWNoRelinquish Control	023	Ein NLM-Modul hat die Kontrolle nicht abgegeben.	critical
sniNWOpenScreen	020	Am Server wurde ein Bildschirm geöffnet.	informational
sniNWProtocolBind	033	Ein Protokoll wurde in einen MLID eingebunden.	informational
sniNWProtocolUnbind	034	Ein Protokoll wurde von einem MLID entfernt.	warning
sniNWQueueAction	043	Eine Warteschlange wurde aktiviert, deaktiviert, erzeugt oder gelöscht.	informational
sniNWRenameObject	048	Für den Verzeichnis-Service (NetWare) wurde ein Objekt umbenannt.	informational
sniNWSysVolume Dismounted	001	SYS-Datenträger wurde vom Server getrennt.	critical
sniNWThreadSwitch	025	Ein Thread-Wechsel ist erfolgt.	informational
sniNWTrusteeChange	019	Für den Server wurde der Verwalter geändert.	informational
sniNWUpdateCursor	016	Die Cursorposition wurde aktualisiert.	informational

Tabelle 49: Threshold-Traps

Trap-Name	ID	Bedeutung	Fehlerklasse
sniNWUpdateScreen	015	Ein Bildschirm wurde aktualisiert.	informational
sniNWValueChanged	049	Der Wert für ein Objekt des Verzeichnis-Service (NetWare) wurde geändert.	informational
sniNWVolSysMounted	000	SYS-Datenträger wurde verbunden.	informational
sniNWVolume Dismounted	003	Datenträger wurde vom Server getrennt.	informational
sniNWVolumeMounted	002	Datenträger wurde verbunden.	informational

Tabelle 49: Threshold-Traps

5.3.24 USV-Traps (Upsman.mib)

MIB-OID: 1.3.6.1.4.1.1356

Im Folgenden finden Sie eine alphabetische Übersicht über die USV-Traps.

USV-Traps 1

Trap-Name	ID	Bedeutung	Fehlerklasse
communication Established	4	Die Verbindung mit der USV wurde hergestellt.	informational
communicationLost	1	Die Verbindung mit der USV wurde getrennt.	critical
powerRestored	5	Die USV wird wieder durch die reguläre Stromversorgung versorgt.	informational
testCompleted	8	Der Test der USV wurde abgeschlossen.	informational
testStarted	7	Der Test der USV wurde gestartet.	informational
upsOnBattery	6	Das USV-System hat auf Batterieversorgung geschaltet.	major
upsOverload	2	Die USV hat eine mehr als hundertprozentige Auslastung ihrer Kapazität festgestellt.	critical
upsTurnedOff	3	Die USV wurde vom Manager abgeschaltet.	major

Tabelle 50: USV-Traps 1

USV-Traps 2

Trap-Name	ID	Bedeutung	Fehlerklasse
boostOn	6	Die USV hat den Verstärker eingeschaltet.	major
communication Established	8	Die Verbindung mit der USV wurde hergestellt.	informational
communicationLost	1	Die Verbindung mit der USV wurde getrennt.	critical
lowBattery	7	Batterien sind schwach und werden bald leer sein.	critical
powerRestored	9	Die USV wird wieder durch die reguläre Stromversorgung versorgt.	informational
returnFromLowBattery	11	Die USV ist aus dem lowBattery-Zustand zurückgekehrt; Batterien sind in Ordnung.	informational
upsDiagnosticsFailed	3	Das USV-System hat seinen internen Selbst-Test mit Fehler beendet.	critical
upsDiagnosticsPassed	10	Das USV-System hat seinen internen Selbst-Test erfolgreich abgeschlossen.	informational
upsDischarged	4	Das USV-System hat soeben eine Laufzeit-Kalibrierung angestoßen.	critical
upsOnBattery	5	Das USV-System hat auf Batterieversorgung geschaltet.	major
upsOverLoad	2	Die USV hat eine mehr als hundertprozentige Auslastung ihrer Kapazität festgestellt.	critical
upsRebootStarted	15	Die USV hat den Reboot gestartet.	major

Tabelle 51: USV-Traps 2

Trap-Name	ID	Bedeutung	Fehlerklasse
upsSleeping	13	Die USV wechselt in den Sleep-Modus.	major
upsTurnedOff	12	Die USV wurde vom Manager abgeschaltet.	major
upsWokeUp	14	Die USV ist aus dem Sleep-Modus zurückgekehrt.	informational

Tabelle 51: USV-Traps 2

6 MIB-Integration

Bei der Installation des Event Managers unter Windows und Linux wird automatisch das Web-basierte Tool **MIB Manager** mit installiert.

Mit dem Tool können fremde MIBs in den Event Manager integriert werden, so dass deren Traps vom Event Manager erkannt werden. Beim Eintreten eines Ereignisses kann dann darauf entsprechend reagiert werden.

Das nachfolgende Beispiel zeigt das Format, das eine Beschreibung von TRAP-Type haben kann, wobei TRAP-Type dabei das Format SMIv1 haben muss.

```
testTrap TRAP-TYPE
ENTERPRISE sniServerMgmt
VARIABLES {
trapServerName,
trapTime
}
DESCRIPTION
"Test trap to verify trap connection."
--#TYPE "Test trap"
--#SUMMARY "Test trap from server %s (no error)."
--#ARGUMENTS { 0 }
--#SEVERITY INFORMATIONAL
--#TIMEINDEX 1
--#HELP "Note: This is no error condition."
--#HELPTAG
--#STATE OPERATIONAL
::= 600
```

Bei der dargestellten MIB Datei wird nur ein Enterprise-String unterstützt.

Beachten Sie:

- Die Namenserweiterung der MIB-Datei muss **.mib** sein.
- Integrierte MIB-Dateien können nicht entfernt werden.
- MIB-Dateien, die Multi-Byte-Zeichen enthalten, werden nicht unterstützt.

MIB Manager starten

Das Tool **MIB Manager** wird folgendermaßen gestartet:

- Wählen Sie im Menü **EVENT MANAGEMENT** den Eintrag **MIB INTEGRATOR**.

Nach dem Starten wird folgendes Fenster angezeigt:

Bild 17: Web-basiertes Tool „MIB Manager“

Gehen Sie wie folgt vor, um fremde MIBs zu integrieren:

- Wählen Sie über die Schaltfläche **Browse...** das entsprechende Verzeichnis aus.
- Wählen Sie die MIB aus und klicken Sie dann auf die Schaltfläche **Upload**. Anschließend überprüft das Tool die MIB auf korrekte Syntax hin. Im nächsten Fenster wird anhand einer Meldung der Status angezeigt.
- Wählen Sie die Schaltfläche **Save parsed MIB**, um die MIB zu integrieren.
- Wählen Sie im nächsten Fenster **Close**, um das Tool zu beenden.

Nachdem eine fremde MIB integriert wurde, muss der Cache des Java-Plugins gelöscht werden. Unter Windows muss der Dienst **ServerView Services** neu gestartet werden. Unter Linux genügt der Neustart des Dienstes **SV Services** mit:
`/usr/bin/sv_services restart`.

Integrierte MIB-Dateien ansehen

Welche MIBs im Event Manager integriert sind, erfahren Sie über das Fenster **Alarm Configuration** (in der Spalte **MIB** in dem Dialogfenster **Alarm Rules - Assign Alarms**) oder über die Online-Hilfe des Event Managers.

Eine ausführliche Beschreibung, wie Sie in das MIB-Übersichtsfenster über die Hilfe gelangen, finden Sie im Abschnitt "Trap-Information abfragen" auf Seite 89 beschrieben.

Aktualisieren von integrierten MIB-Dateien

Sie können integrierte MIB-Dateien aktualisieren. Der Name der aktualisierten integrierten MIB-Datei muss dabei gleich dem Namen der integrierten MIBDatei sein.

Beachten Sie, dass der MIB-Integrator zwischen Groß- und Kleinschreibung unterscheidet.